IBM SecureWay Trust Authority

Systemverwaltung

Version 3 Release 1.2

SH12-2979-01

IBM SecureWay Trust Authority

Systemverwaltung

Version 3 Release 1.2

SH12-2979-01

Anmerkung

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter „Bemerkungen" auf Seite 123 gelesen werden.

Zweite Ausgabe (Juni 2000)

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM SecureWay Trust Authority System Administration Guide,
IBM Form SH09-4532-01,

herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 2000
© Copyright IBM Deutschland Informationssysteme GmbH 2000

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW NLS Center
Kst. 2877
Juni 2000

Inhaltsverzeichnis

Tabellen v

Kapitel 1. Informationen zu Trust Authority 1

Kapitel 2. Übersicht 3

Kapitel 3. Informationen zur Vorgehensweise 5

Trust Authority verwalten 5
- Befehle unter Windows NT eingeben 5
- Trust Authority-Kennwörter ändern 5
- Server-Komponenten starten und stoppen . . . 7
- IniEditor zum Ändern von Konfigurationsdateien verwenden 9
- Trust Authority-IP-Adressen ändern 11
- System sichern und wiederherstellen 12
- Anzahl von Benutzern und Zertifikaten überwachen 13
- Zertifikatsaktivität überwachen 14

WebSphere Application Server verwalten 16
- Status des WebSphere Application Server prüfen 16
- WebSphere Application Server-Protokolle prüfen 16

HTTP Server verwalten 17
- Status des HTTP Server prüfen 17
- HTTP Server-Protokolle prüfen 19

CA-Server verwalten 20
- Vom CA-Server überwachten Anschluß ändern 21
- CA-Sendeaufrufintervall ändern 21
- CRL-Einstellungen ändern 22
- ICL-Schutzregel ändern 23
- ICL-Schutzschlüssel ändern 24
- Integrität der CA-Server-Datenbank prüfen . . . 24
- CA-Zertifikat mit Hilfe gegenseitiger Zertifizierung anfordern 25
- CA-Zertifikat mit Hilfe des Hierarchiemodells anfordern 28
- CA-Server-Protokolle prüfen. 32
- CA-Server-Status prüfen 32
- Aktivierung der CRL-Verteilungspunkte 33

CA-Server verwalten 34
- Registratoren hinzufügen 34
- Verschlüsselung für die RA-Datenbank aktivieren 37
- Vom RA-Server überwachten Anschluß ändern 38
- RA-Sendeaufrufintervall ändern 38
- RA-Wiederholungsintervall ändern 39
- RA-Server-Protokolle prüfen. 39
- RA-Server-Status prüfen 39
- RA-Einstellungen für die Kommunikation mit dem Directory ändern 41

Prüfsubsystem verwalten 42
- Protokolleinträge anzeigen 43
- Protokolleinträge suchen 46
- Prüf-Server-Anschluß im Prüf-Client ändern . . 46
- Sendeweise für Ereignisse vom Prüf-Client ändern 47
- Vom Prüf-Server überwachten Anschluß ändern 48
- Anzahl der Bindungsversuche zwischen Prüf-Server und Prüf-Client ändern 49
- Intervall zwischen Bindungsversuchen ändern. . 49
- Protokolleinstellungen ändern 49
- Prüfberichte generieren 52
- Prüfprotokolldateien archivieren und unterzeichnen 52
- Integrität der Datenbank des Prüf-Servers und der Archivierungsdateien prüfen 53
- Status des Prüf-Servers prüfen 55
- Prüf-Server-Protokolle prüfen 56

DB2-Datenbanken verwalten. 57
- Status von DB2-Datenbanken prüfen 57
- DB2-Protokolle prüfen. 59

Directory-Server verwalten 59
- Directory-Server-Status prüfen 60
- Directory-Server-Protokolle prüfen. 61

IBM SecureWay 4758 PCI Cryptographic Coprocessor verwalten. 61

Kapitel 4. Erläuterungen 63

Trust Authority - Sicherheit 63

Zugriffssteuerungslisten 63

Zertifikatsaussteller. 63
- CA-Hierarchien 64
- Zertifikatserweiterungen 64
- Zertifikatwiderrufslisten 67
- Gegenseitige Zertifizierung 68

Zertifizierung. 68
- Digitale Zertifikate 68
- Registrierte Namen. 69
- Liste der ausgestellten Zertifikate (CRL) 69
- Unterzeichnen und Gültigkeitsprüfung für Unterschriften 69

Registrierungsstellen (RA) 70
- Registratoren 70
- Registrierungsdomänen 70

IBM SecureWay 4758 PCI Cryptographic Coprocessor 70

Smart Cards 71

Prüfung 72
- Protokolleinträge 72
- Prüfereignisse 72
- Masken für Prüfereignisse 73
- Verbindliche und wahlfreie Prüfereignisse . . . 73
- Integritätsprüfung 73
- Integritätsversiegelung. 73
- Archivieren von Prüfprotokollen 73

DB2-Datenbanken 73

Web-Server 74
- IBM WebSphere Application Server 74
- IBM HTTP Server 74

IP-Aliasing 75
Directory-Server 75
Objektkennungen 76

Kapitel 5. Referenzinformationen . . . 77
Konfigurationsdateien 77
Dateibeschreibung 77
CA-Server - Konfigurationsdatei 78
RA-Server - Konfigurationsdatei 87
Prüf-Server - Konfigurationsdatei 97
Prüf-Client-Konfigurationsdatei AuditClient.ini 101
Befehlszeilendienstprogramme. 103
Dienstprogramm CA Certification 103
Dienstprogramm Add RA User 105
Dienstprogramm Enable RA Database Encryption. 106
Dienstprogramm Audit Archive and Sign . . . 107
Dienstprogramm Audit Integrity Check . . . 107
Felder für Prüfereignisse 109
Prüfereignisse 110
Daten der Prüfdatenbank 113
Schlüsseltabelle 114
Tabelle für Ereignisbewertung 114
Tabelle zur Ereignissteuerung 114
Quellentabelle 115
Tabelle der berechtigten Entitäten. 115
Tabelle der berechtigten Aufgabenbereiche. . . 116
Tabelle der Arten betroffener Entitäten 116
Tabelle der Komponentenarten 116
Prüfprotokolltabelle 117
Systemtabelle 118
Fehlerbehebung 120
Grundlegende Fehlerbehebung 120
Fehlerbehebung mit aktivierter Nachrichtenerstellung auf Debug-Stufe 121

Bemerkungen 123
Marken und Dienstleistungsmarken 124

Bezugsinformationen 127

Glossar 129

Index 143

Tabellen

1. Trust Authority-Konfigurationsdateien . . . 10
2. WebSphere Application Server-Protokolle über Transaktionen mit dem Setup Wizard 16
3. IBM WebSphere Application Server - Protokolle über Transaktionen mit der Registrierungsanwendung 17
4. HTTP Server-Protokolle über Transaktionen mit dem Setup Wizard 19
5. HTTP Server-Protokolle über Transaktionen mit Ihrer Registrierungsanwendung 19
6. Protokolle des CA-Servers 32
7. RA-Server-Protokolle 39
8. Spaltenbeschreibungen der Sichten für die Trust Authority-Prüfdatenbank 44
9. Protokolle des Prüf-Servers 56
10. Datenbankpositionen 57
11. Protokolle des Directory-Servers 61
12. Zertifikatserweiterungen 65
13. Modell für IBM HTTP Server mit drei Servern und drei Anschlüssen 75
14. CA-Server - Konfigurationsdatei 79
15. RA-Server - Konfigurationsdatei 88
16. Prüf-Server - Konfigurationsdatei 98
17. Prüf-Client - Konfigurationsdatei 102
18. Felder für Prüfereignisse 109
19. Prüfereignisse 110
20. Felder der Schlüsseltabelle 114
21. Felder in der Tabelle für die Ereignisbewertung 114
22. Felder in der Tabelle für die Ereignissteuerung 114
23. Felder in der Quellentabelle 115
24. Felder in der Tabelle berechtigter Entitäten 115
25. Felder in der Tabelle berechtigter Aufgabenbereiche 116
26. Felder in der Tabelle der Arten betroffener Entitäten 116
27. Felder in der Tabelle der Komponentenarten 116
28. Felder in der Prüfprotokolltabelle 117
29. Felder in der Systemtabelle 118

Kapitel 1. Informationen zu Trust Authority

IBM SecureWay Trust Authority ermöglicht Anwendungen das Authentifizieren von Benutzern und das Bereitstellen gesicherter Kommunikation:

- Unternehmen können digitale Zertifikate in Übereinstimmung mit ihren Registrierungs- und Zertifizierungsrichtlinien ausstellen, veröffentlichen und verwalten.
- Unterstützung für PKIX- (Public Key Infrastructure for X.509 Version 3) und CDSA-Verschlüsselungsstandards (CDSA = Common Data Security Architecture) zur Realisierung der Interoperabilität zwischen verschiedenen Lieferanten und Herstellern.
- Digitale Unterzeichnung und gesicherte Protokolle zur Authentifizierung aller an einer Transaktion beteiligten Parteien.
- Optimale Flexibilität durch browser- und client-basierte Registrierungsfunktionen.
- Gewährleistung der Vertraulichkeit durch verschlüsselte Kommunikation und gesicherte Speicherung der Registrierungsinformationen.

Ein Trust Authority-System kann auf IBM AIX/6000- und Microsoft Windows NT-Server-Plattformen ausgeführt werden. Es umfaßt die folgenden wichtigen Funktionen:

- Ein zuverlässiger Zertifikatsaussteller (CA) verwaltet die gesamte Gültigkeitsdauer digitaler Zertifikate. Zur Bestätigung der Richtigkeit eines Zertifikats, unterzeichnet der CA alle von ihm ausgestellten Zertifikate digital. Außerdem unterzeichnet er Zertifikatswiderrufslisten (CRLs), um zu bestätigen, daß ein bestimmtes Zertifikat nicht mehr gültig ist. Zur weiteren Sicherung seines Unterschriftsschlüssels können Sie kryptografische Hardware, z. B. den IBM SecureWay 4758 PCI Cryptographic Coprocessor, einsetzen.
- Eine Registrierungsstelle (RA) führt die Verwaltungsaufgaben aus, die bei der Benutzerregistrierung notwendig sind. Sie stellt sicher, daß nur solche Zertifikate ausgestellt werden, die Ihre Unternehmensaktivitäten unterstützen, und daß diese Zertifikate nur an berechtigte Benutzer ausgegeben werden. Die Verwaltungsaufgaben können über automatisierte Prozesse oder auf der Basis menschlicher Entscheidungen ausgeführt werden.
- Eine Web-Schnittstelle für die Registrierung vereinfacht das Abrufen von Zertifikaten für Browser, Server und andere Einheiten und Zwecke, z. B. VPN-Einheiten (VPN = Virtual Private Network), Smart Cards und die sichere Übertragung von E-Mails.
- Eine Windows-Anwendung, der Trust Authority-Client, ermöglicht Endbenutzern das Abrufen und Verwalten von Zertifikaten ohne einen Web-Browser.
- Eine Web-Verwaltungsschnittstelle, das RA Desktop, ermöglicht berechtigten Registrierungsstellen die Genehmigung oder Zurückweisung von Registrierungsanforderungen sowie die Verwaltung von Zertifikaten nach deren Ausstellung.
- Ein Prüfsubsystem ermittelt einen Nachrichtenauthentifizierungscode (MAC) für jeden Protokolleintrag. Wenn Prüfdaten nach ihrer Aufzeichnung in der Prüfdatenbank geändert oder gelöscht werden, können Sie mit Hilfe des MAC diese Manipulation feststellen.
- Regel-Exits ermöglichen Anwendungsentwicklern die Anpassung der Registrierungsprozesse.

- Integrierte Unterstützung für eine Verschlüsselungsmaschine. Zur Authentifizierung der Kommunikation werden die Trust Authority-Hauptkomponenten mit einem werkseitig generierten, privaten Schlüssel unterzeichnet. Sicherheitsobjekte, z. B. Schlüssel und MACs, werden verschlüsselt und in geschützten Bereichen (sogenannten KeyStores oder Schlüsselspeichern) gespeichert.
- Integrierte Unterstützung für IBM SecureWay Directory. Das Directory speichert Informationen zu gültigen und zurückgewiesenen Zertifikaten in einem LDAP-kompatiblen Format.
- Integrierte Unterstützung für IBM WebSphere Application Server und IBM HTTP Server. Der Web-Server arbeitet mit dem RA-Server, um Nachrichten zu verschlüsseln, Anforderungen zu authentifizieren und Zertifikate an den gewünschten Empfänger zu übertragen.
- Integrierte Unterstützung für das ausgezeichnete IBM Produkt DB2 Universal Database.

Kapitel 2. Übersicht

Dieses Dokument enthält die erforderlichen Informationen für Betrieb und Verwaltung des Trust Authority-Systems. Es wird vorausgesetzt, daß Sie in den folgenden Bereichen über ausreichende Kenntnisse verfügen:

- Betriebssystem AIX oder UNIX
- Betriebssystem Windows NT
- Systemarchitektur
- Netzverwaltung
- Datenbankverwaltung
- Web-Server-Verwaltung
- Verzeichnisverwaltung

„Kapitel 3. Informationen zur Vorgehensweise" auf Seite 5, enthält Informationen zu Betrieb und Verwaltung des Trust Authority-Systems. Hier erfahren Sie, wie Sie das System starten und stoppen, Kennwörter ändern, den Editor für Konfigurationsdateien verwenden, das System sichern und wiederherstellen und folgende Systemkomponenten verwalten können:

- IBM WebSphere Application Server
- IBM HTTP Server
- CA-Server
- RA-Server
- Prüfsubsystem
- IBM DB2 Universal Database (UDB)
- IBM SecureWay Directory
- IBM SecureWay 4758 PCI Cryptographic Coprocessor

„Kapitel 4. Erläuterungen" auf Seite 63, enthält detaillierte technische Informationen zu den Themen, die bei der Beschreibung der Prozeduren angesprochen werden.

Der Abschnitt „Kapitel 5. Referenzinformationen" auf Seite 77 enthält Referenzinformationen, beispielsweise Parameter von Konfigurationsdateien, die Syntax von Befehlszeilendienstprogrammen sowie Informationen in Tabellenform zum Prüfsubsystem.

Kapitel 3. Informationen zur Vorgehensweise

Die Abschnitte in diesem Kapitel erläutern, wie Sie IBM SecureWay Trust Authority und dessen Komponenten verwalten.

Trust Authority verwalten

in diesem Abschnitt werden die Tools und Prozesse beschrieben, die Sie zur Verwaltung des gesamten Trust Authority-Systems verwenden können.

Folgende Arbeitsschritte werden erläutert:

- Eingabe von Befehlen über die Windows NT-Befehlszeile
- Ändern von Trust Authority-Kennwörtern
- Starten und Stoppen der Server-Komponenten
- Verwenden des Programms IniEditor zum Ändern von Konfigurationsdateien
- Prüfen der Trust Authority-Konfigurationsprotokolle
- Ändern von Trust Authority-IP-Adressen
- Sichern und Wiederherstellen des Systems
- Überwachen der Zertifikatsaktivität
- Aufzeichnen der Anzahl von Benutzern und Zertifikaten

Befehle unter Windows NT eingeben

Wenn Sie Trust Authority unter Windows NT installiert haben, gibt es für eine Reihe von Tasks keine Programmsymbole, so daß diese Tasks von einer DOS-Befehlszeile aus aufgerufen werden müssen. So muß beispielsweise add_rauser manuell ausgeführt werden, damit Registratoren definiert werden können.

Wenn Sie einen Befehl angeben, für den ein Verzeichnispfad als Parameter erforderlich ist, und dieser Pfad eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (″) setzen. So muß beispielsweise der Parameter für den Pfad im Befehl add_rauser wie folgt angegeben werden:

```
add_rauser "c:\Program Files\IBM\Trust Authority\bin"
```

Trust Authority-Kennwörter ändern

IBM Trust Authority verfügt über ein Dienstprogramm zum Ändern von Kennwörtern. Mit diesem Dienstprogramm können Sie die während der Konfiguration des Systems definierten Standardkennwörter ändern. Ändern Sie die Kennwörter mindestens einmal nach der ersten Konfiguration des Systems und bevor Sie das System Ihren Benutzern zur Verfügung stellen. Diese Kennwörter ermöglichen den Zugriff auf folgende Funktionskomponenten:

- Sicherer Startmechanismus

  Das Kennwort für das Steuerprogramm ermöglicht dem System, alle Trust Authority-Komponenten automatisch zu starten oder herunterzufahren. Außerdem kann mit diesem Kennwort auf den sicheren Start-Chiffrierschlüssel zugegriffen werden.
- Directory

  Das Directory-Administratorkennwort steuert den Zugriff auf änderbare Elemente im Directory.

- Prüf-Server

  Das Prüfadministratorkennwort ermöglicht den Zugriff auf Prüfprotokolle und Verwaltungs-Tools für Prüfoperationen.
- CA-Profil für IBM 4758

  Das CA-Profilkennwort für IBM 4758 steuert den Zugriff auf das CA-Profil des IBM SecureWay 4758 PCI Cryptographic Coprocessor.

Zum Ändern von Kennwörtern stehen Ihnen verschiedene Methoden zur Verfügung. Wenn Sie Trust Authority auf einer AIX-Plattform installiert haben, müssen Sie die unter „Befehlszeilenprozedur" beschriebene Befehlszeilenprozedur verwenden. Wenn Sie das Produkt auf einer Windows NT-Plattform ausführen, können Sie entweder die unter „Vorgehensweise anhand von Programmsymbolen unter Windows NT" auf Seite 7 beschriebene Prozedur oder die Befehlszeilenprozedur verwenden, um das Dienstprogramm 'Change Password' auszuführen.

Befehlszeilenprozedur

1. Wechseln Sie in das Trust Authority-Verzeichnis 'bin', indem Sie einen der folgenden Pfade eingeben:
   - Unter AIX lautet der Standardpfad:

     `/usr/lpp/iau/bin`
   - Unter Windows NT lautet der Standardpfad:

     `c:\Program Files\IBM\Trust Authority\bin`
2. Geben Sie je nach Betriebssystem einen der folgenden Befehle ein:
   - Unter AIX:

     changePWD.sh
   - Unter Windows NT:

     changePWD.bat

   Das folgende Menü wird angezeigt:

   ```
   ------------- Change Trust Authority Passwords --------------
   Enter the option number for the component you want to change.
   You will be prompted to enter the current password and then
   the new password.
   ---------------------------------------------------------------
   Change password for
   1) Quit
   2) Control Program
   3) Directory Administrator
   4) Audit Administrator
   5) 4758 CA Profile
   Enter Option:
   ```
3. Wählen Sie die Option für das zu ändernde Kennwort aus, indem Sie im Feld Option eingeben die entsprechende Zahl eingeben.
4. Geben Sie nach Aufforderung das aktuelle Kennwort für die ausgewählte Option ein, und bestätigen Sie es.

   Anmerkungen:

   a. Bei der erstmaligen Nutzung dieses Tools müssen Sie als aktuelles Kennwort das Kennwort eingeben, das bei der Konfiguration des Systems definiert wurde. Geben Sie bei Kennwörtern für das Steuerprogramm und für Prüfadministratoren das Kennwort des Trust Authority-Servers als aktuelles Kennwort ein. Geben Sie für das Kennwort des Directory-Administrators das bei der Konfiguration als aktuelles Kennwort definierte Kennwort ein. Geben Sie für das 4758-CA-Profil das Kennwort **IBMCA001** an.

b. Wenn Sie Trust Authority auf einem AIX-Server installiert haben und das Kennwort des Konfigurationsbenutzers (cfguser) vor dem Konfigurieren des Systems nicht geändert wurde, lautet das Standardkennwort **Secure99**.

5. Geben Sie nach Aufforderung das aktuelle Kennwort für die ausgewählte Option ein, und bestätigen Sie es.

   Das Kennwort darf maximal acht Zeichen lang sein (das 4758-CA-Profilkennwort muß exakt acht Zeichen lang sein).

   Das Dienstprogramm zeigt bei erfolgreicher Änderung eine entsprechende Nachricht an.

Nach dem erfolgreichen Abschluß der Verarbeitung ruft das Dienstprogramm das Hauptmenü erneut auf.

Vorgehensweise anhand von Programmsymbolen unter Windows NT

Wenn Sie Trust Authority auf einer Windows NT-Plattform ausführen und das Auswählen von Programmsymbolen gegenüber der Befehlseingabe in einem DOS-Befehlsfenster bevorzugen, können Sie anhand der folgenden Prozedur das Dienstprogramm 'Change Password' ausführen:

1. Wählen Sie nacheinander **Start → Programme → IBM SecureWay Trust Authority → Change Passwords Tool** aus.

   Das Menü 'Trust Authority-Kennwörter ändern' wird angezeigt.

2. Führen Sie die Schritte aus, beginnend mit 3 auf Seite 6 unter „Befehlszeilenprozedur" auf Seite 6.

Server-Komponenten starten und stoppen

IBM Trust Authority verwendet einen sicheren, automatischen Startmechanismus, der als Trust Authority-Steuerprogramm bezeichnet wird, um alle Komponenten einer Maschine zu starten oder zu stoppen. Die Trust Authority-Steuerung (im Falle ferner Maschinen eine pro Maschine) verfügt über einen eigenen Chiffrierschlüssel, mit dem Komponentenkennwörter bei Bedarf ver- oder entschlüsselt werden. Wenn Sie Trust Authority-Server-Komponenten auf fernen Maschinen installiert haben, finden Sie im Abschnitt „Ferne Server starten und stoppen" auf Seite 9 weitere Informationen.

Server-Komponenten lokal starten und stoppen

Um alle Komponenten einer Maschine zu starten oder zu stoppen, können Sie eine der folgenden Methoden verwenden:

- Geben Sie die folgenden Befehle unter AIX ein, um die Server-Komponenten zu starten oder zu stoppen. Befolgen Sie die Online-Anweisungen zur Eingabe des Kennworts für das Steuerprogramm. Beachten Sie, daß Sie sich als Trust Authority-Konfigurationsbenutzer (cfguser) anmelden müssen, um das System zu starten. Um das System zu stoppen, können Sie sich als 'root' oder als 'cfguser' anmelden.

  ```
  cd /usr/lpp/iau/bin
  Start_TA.sh
  oder
  Stop_TA.sh
  ```

- Wenn Sie Trust Authority auf einer Windows NT-Plattform installiert haben, können Sie das entsprechende Symbol im Windows NT-Programmenü auswählen. Sie können beispielsweise folgendes auswählen:

  ```
  Start > Programme > IBM SecureWay Trust Authority > Trust Authority startenStart >
  Programme > IBM SecureWay Trust Authority > Trust Authority stoppen
  ```

- Wenn Sie unter Windows NT die Befehlseingabe verwenden möchten, geben Sie die folgenden Befehle in einer DOS-Befehlszeile ein, um die Server-Komponenten zu starten bzw. zu stoppen. Befolgen Sie die Online-Anweisungen zur Eingabe des Kennworts für das Steuerprogramm.

  ```
  Start_TA.bat
  oder
  Stop_TA.bat
  ```

Richtlinien zur Verwendung unter AIX: Die Richtlinien zum Starten und Stoppen des Systems unter AIX sehen folgendermaßen aus:

- Wenn der CA- und der RA-Server durch die Ausführung des Steuerprogramms unter AIX nicht gestoppt werden können, müssen Sie den Befehl 'ps' verwenden, um die aktiven httpd-Prozesse aufzulisten, und diese anschließend mit dem Befehl 'kill' stoppen. Nachfolgend sind Beispiele für die Verwendung dieser Befehle sowie Beispiele für Ausgabedaten aufgeführt.

  ```
  $ ps -ef | grep irgAutoCA
  root 18886     1   0   Oct 24      - 76:34 /usr/lpp/iau/bin/irgAutoCa
     /usr/lpp/iau/etc/TrustAuthority/irgAutoCA.ini
  cfguser 23316 32400   2 11:58:20  pts/4  0:00 grep irgAutoCA
  $ kill 18886
  $ ps -ef | grep irgrasvr
  root 23526     1  12   Oct 24      - 207:46 /usr/lpp/iau/bin/irgrasvr -c
     /usr/lpp/iau/pkrf/etc/domain.cfg -d YourDomain
  cfguser 26016 12488   3 11:57:16  pts/0  0:00 grep irgrasvr
  $ kill 23526
  ```

- Durch das Stoppen von Trust Authority werden die Web-Server-Programme unter AIX normalerweise automatisch gestoppt. Ist dies nicht der Fall, können Sie den Befehl 'ps' verwenden, um die Prozeß-ID des für die jeweilige Domäne zu stoppenden Exemplars festzustellen, und dieses Exemplar anschließend mit dem Befehl 'kill' stoppen. Beispiel:

  ```
  ps -ef | grep OutOfProc | grep YourDomain
  kill Prozeß-ID
  ```

- Durch das Starten und Stoppen von Trust Authority wird auch der Directory-Server automatisch gestartet bzw. gestoppt. Wenn das Directory nicht automatisch gestartet bzw. gestoppt werden soll, müssen Sie den Abschnitt [AutoStopN] der Datei 'TrustAuthControl.cfg' editieren, um den Eintrag für die Directory-Komponente zu entfernen.

Richtlinien zur Verwendung unter Windows NT: Die Richtlinien zum Starten und Stoppen des Systems unter Windows NT sehen folgendermaßen aus:

- Durch das Stoppen von Trust Authority werden die Web-Server-Programme unter Windows NT nicht automatisch gestoppt. Nach dem Stoppen von Trust Authority müssen Sie das WebSphere-Exemplar, das für die Registrierungsdomäne gestartet wurde, manuell stoppen. Verwenden Sie hierzu den Windows NT-Task-Manager, um den java.exe- und den reqdbagent.exe-Prozeß zu beenden.
- Um eine optimale Leistung zu erhalten, sollten Sie vor einem erneuten Starten der Server-Komponenten auf einem Windows NT-System einen Neustart der Maschine durchführen.
- Wenn Sie das Steuerprogramm verwenden, um die Trust Authority-Server-Komponenten unter Windows NT zu starten, kann das Fenster, in dem das Programm gestartet wird, nicht geschlossen werden. Dies liegt daran, daß einige Komponenten diesem Konsolfenster zugeordnet sind. Nach dem Stoppen der Trust Authority-Server-Komponenten kann auch dieses Fenster geschlossen werden.
- Durch das Starten und Stoppen von Trust Authority wird auch der Directory-Server automatisch gestartet bzw. gestoppt. Wenn das Directory nicht automa-

tisch gestartet bzw. gestoppt werden soll, müssen Sie den Abschnitt [AutoStopN] der Datei 'TrustAuthControl.cfg' editieren, um den Eintrag für die Directory-Komponente zu entfernen.

Ferne Server starten und stoppen

Wenn Sie die Trust Authority-Komponenten auf fernen Maschinen installiert haben, müssen Sie das Steuerprogramm verwenden, um die Komponenten auf den einzelnen Maschinen zu starten oder zu stoppen. Verwenden Sie zum Starten ferner Komponenten die folgende Reihenfolge:

1. Directory-Server
2. CA- und Prüf-Server
3. RA-Server (einschließlich IBM HTTP Server und WebSphere Application Server)

Zum Stoppen des Systems müssen die Server-Programme in der umgekehrten Reihenfolge gestoppt werden.

IniEditor zum Ändern von Konfigurationsdateien verwenden

In diesem Abschnitt wird beschrieben, wie Sie den Editor für Konfigurationsdateien IniEditor aufrufen und verwenden. Mit dem Tool IniEditor können Sie Parameter in allen Abschnitten der IBM Trust Authority-Konfigurationsdateien hinzufügen, aktualisieren und löschen. Alle Parameter werden in einem Editierfeld in der Form Name=Wert angezeigt, damit Sie die zu ändernden Bereiche schnell lokalisieren und editieren können. Informationen zu Parametern und deren Nutzung finden Sie im Abschnitt „Konfigurationsdateien" auf Seite 77.

Anmerkungen:

1. IniEditor ist ein einfacher Editor zum Editieren von Konfigurationsdateien. Das Tool bietet keine Funktionen zur Gültigkeitsprüfung von Daten.
2. Sichern Sie zu Ihrem eigenen Schutz die zu editierenden Konfigurationsdateien, bevor Sie Änderungen vornehmen.

Editor starten

Sie können den Editor über die Eingabeaufforderung mit oder ohne Angabe der zu editierenden Datei starten.

Geben Sie einen der beiden folgenden Befehle ein, um den Editor mit der Datei meinedat.ini zu starten:

- In der Befehlszeile der AIX-Umgebung:

```
cd /usr/lpp/iau/bin
run_IniEditor meinedat.ini
```

- In der DOS-Befehlszeile der Windows NT-Umgebung:

```
cd c:\Program Files\IBM\Trust Athority\bin
IniEditor meinedat.ini
```

Geben Sie einen der beiden folgenden Befehle ein, um den Editor ohne Angabe eines Dateinamens zu starten:

- In der Befehlszeile der AIX-Umgebung:

```
run_IniEditor
```

- In der DOS-Befehlszeile der Windows NT-Umgebung:

```
IniEditor
```

Wenn Sie keinen Dateinamen eingeben, werden Sie gefragt, ob Sie eine neue oder eine vorhandene Datei editieren wollen. Handelt es sich um eine neue Datei, wer-

den Sie zur Eingabe des Dateityps aufgefordert. Für jeden Dateityp existiert eine entsprechende Schablone (Ini-Datei), die nach Angabe des Dateityps eingelesen wird. Folgende Optionen sind möglich:

Tabelle 1. Trust Authority-Konfigurationsdateien

AIX-Standardpfad	Windows NT-Standardpfad	Beschreibung
/usr/lpp/iau/etc/TrustAuthority/ jonahca.ini	c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\jonahca.ini	Die Konfigurationsdatei des CA-Servers. Diese Datei enthält die Konfigurationsvariablen des CA-Servers. Sie können diese Variablen ändern, um grundlegende Funktions-merkmale und Verbindungs-einstellungen festzulegen.
/usr/lpp/iau/pkrf/Domains/ YourDomain/etc/jonahra.ini	c:\Program Files\IBM\Trust Authority \pkrf\Domains\YourDomain\etc\ jonahra.ini	Die Konfigurationsdatei des RA-Servers. Diese Datei enthält die Konfigurationsvariablen des RA-Servers. Neben den grundlegenden Funktions-merkmalen und Verbindungs-einstellungen ermöglichen diese Variablen die Steuerung der Interaktion von RA- und Directory-Server.
/usr/lpp/iau/etc/AuditClient.ini	c:\Program Files\IBM\Trust Authority\etc\AuditClient.ini	Die Konfigurationsdatei des Prüf-Clients. Diese Datei enthält die Konfigurationsvariablen der Prüf-Clients. Die Variablen ermöglichen Verbindungs-einstellungen und unterstützen die Optimierung der Prüfmaske, die die Weiterleitung von Prüf-ereignissen steuert.
/usr/lpp/iau/etc/TrustAuthority/AuditServer.ini	c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\ AuditServer.ini	Die Konfigurationsdatei des Prüf-Servers. Diese Datei enthält die Konfigurationsvariablen des Prüf-Servers. Sie können diese Variablen ändern, um grundlegende Funktions-merkmale und Verbindungs-einstellungen des Prüf-Servers neu zu konfigurieren und um das Protokollieren von Debug- und Fehlernachrichten zu steuern. Die Variablen legen außerdem fest, welche Ereignisse protokolliert werden.

IniEditor versucht, die Schablonendateien in dem Verzeichnis zu lokalisieren, in dem sich die Trust Authority-Dateien befinden.

Editor verwenden

Nachdem Sie IniEditor mit einer Konfigurationsdatei geladen haben, werden die vorhandenen Parameter auf der linken Seite der Anzeige in Form einer Baumstruktur angezeigt. Diese Struktur enthält die Abschnitte und Schlüssel der Datei. Klicken Sie zum Auswählen eines Abschnitts auf dessen Namen. Klicken Sie auf das Pluszeichen, um einen Abschnitt zu erweitern. Enthält ein Abschnitt Schlüssel, wird der entsprechende Parameter in einem Editierfeld auf der rechten Seite der Anzeige in der Form Name=Wert angezeigt.

Parameter editieren: Sie können folgende Editier-Tasks ausführen:

- Sie können den Wert eines Parameters ändern, indem Sie den Text im Editierfeld überschreiben.
- Wählen Sie zum Widerrufen von Änderungen die Option **Editieren → Rückgängig machen** aus.
- Wählen Sie zum Löschen eines Parameters oder eines Abschnitts die zu löschenden Elemente und anschließend die Option **Editieren → Entfernen** aus.

Abschnitt hinzufügen: Gehen Sie wie folgt vor, um der Ini-Datei einen Abschnitt hinzuzufügen:

1. Wählen Sie die Option **Objekt → Neuer Abschnitt...** aus.

   Das Dialogfenster 'Neuen Abschnitt hinzufügen' wird angezeigt.
2. Geben Sie in diesem Dialogfenster den Namen des Abschnitts an.
3. Klicken Sie auf **OK**.

   Der neue Abschnitt wird am Ende der Baumstruktur angezeigt.

Parameter hinzufügen: Gehen Sie wie folgt vor, um einem Abschnitt der Ini-Datei einen Parameter hinzuzufügen:

1. Wählen Sie die Option **Objekt → Neuer Parameter...** aus.

   Das Dialogfenster 'Einen neuen Parameter erstellen' wird angezeigt. Es enthält ein verdecktes Menü, in dem Sie den Abschnitt auswählen können, dem Sie einen Parameter hinzufügen wollen.
2. Geben Sie im Feld **Parameter** den Namen des Parameters an.
3. Geben Sie im Feld **Wert** den Wert des Parameters an.
4. Klicken Sie auf **OK**.

   Der neue Parameter wird in der Baumstruktur unter dem gewählten Abschnitt und auf der rechten Seite des Fensters in einem Editierfeld angezeigt.

Datei speichern: Mit IniEditor können Sie die aktuelle Ini-Datei unter demselben oder einem anderen Namen speichern oder das Programm beenden. Wurde die Datei geändert, fordert Sie der Editor zum Sichern der Änderungen auf. Sowohl die Option 'Sichern' als auch die Option 'Beenden' (mit Sicherung) speichern die aktuelle Datei als Sicherungskopie mit der Erweiterung .save und überschreiben die alte Datei.

Trust Authority-IP-Adressen ändern

Wurde das Trust Authority-System mit einem einzigen Host-Namen auf einer einzigen Maschine installiert und konfiguriert, können Sie die IP-Adresse dieser Maschine mit folgender Prozedur ändern:

1. Stoppen Sie das Trust Authority-System.
2. Ändern Sie die IP-Adresse der Maschine gemäß den Regeln Ihres Unternehmens.
3. Fahren Sie die Maschine herunter und starten Sie sie erneut.
4. Starten Sie das Trust Authority-System.

Dieses Dokument behandelt keine anderen Szenarien mit mehreren Maschinen, IP-Adressen mit mehreren Host-Namen oder Änderungen von Host-Namen. Informationen zu aktuellen Prozeduren erhalten Sie über die Bibliotheksseite (Library) auf der Web-Site von IBM SecureWay Trust Authority.

System sichern und wiederherstellen

Dieser Abschnitt behandelt die Sicherung und Wiederherstellung von IBM SecureWay Trust Authority. Folgende Themen werden ausführlich behandelt:

- Richtlinien für das Sichern und Wiederherstellen der Trust Authority-Datenbanken.
- Sichern und Wiederherstellen der Betriebssysteme AIX und Windows NT.
- Klonen des IBM SecureWay 4758 PCI Cryptographic Coprocessor

Sichern und Wiederherstellen unter AIX und Windows NT

Um Trust Authority unter AIX oder Windows NT korrekt sichern zu können, müssen Sie zunächst alle Trust Authority-Prozesse in folgender Reihenfolge herunterfahren:

1. Trust Authority
2. DB2-Datenbanken

Datenbanken müssen unabhängig vom verwendeten Sicherungsdienstprogramm heruntergefahren werden. Der Directory-Server und DB2 verwenden asynchrone Schreibzugriffe. Solange diese Prozesse nicht heruntergefahren sind, kann nicht gewährleistet werden, daß die Daten in den Speicherpuffern mitgesichert werden. Je näher Sie das System an einen Einzelbenutzer-Wartungsmodus heranführen, desto besser wird die Datensicherung. Informationen zum Stoppen und Starten von Trust Authority finden Sie im Abschnitt „Server-Komponenten starten und stoppen" auf Seite 7. Informationen zum Stoppen und Starten der Datenbanken finden Sie im Handbuch *IBM DB2 Universal Database Command Reference, Version 5.2*.

Für Sicherungsdienstprogramme empfiehlt IBM folgendes:

- Nutzen Sie unter AIX die systeminternen Sicherungsdienstprogramme 'mksysb' und 'savevg' oder ADSM (ein weiteres IBM Produkt). Die korrekten Prozeduren für die Sicherungsdienstprogramme 'mksysb' und 'savevg' entnehmen Sie bitte Ihrer AIX-Dokumentation. Verwenden Sie ADSM nur gemeinsam mit 'mksysb'.
- Nutzen Sie unter Windows NT ein Produkt, das in der Lage ist, ein Systemabbild zu erstellen, mit dem Sie das gesamte System wiederherstellen können. Verwenden Sie ADSM nur gemeinsam mit mit dem jeweiligen Systemabbild-Dienstprogramm.

Befolgen Sie die Wiederherstellungsanweisungen des jeweiligen Dienstprogramms.

IBM 4758 PCI Cryptographic Coprocessor klonen

Zum Sichern des IBM SecureWay 4758 PCI Cryptographic Coprocessor müssen Sie den Hauptschlüssel der Maschine, auf der das Trust Authority-System installiert ist, auf einer anderen Maschine klonen. Informationen zu den dafür erforderlichen Prozeduren erhalten Sie auf der Seite für die Bibliothek der Web-Site von IBM SecureWay Trust Authority unter folgender Adresse:

`http://www.ibm.com/software/security/trust/library`

Anzahl von Benutzern und Zertifikaten überwachen

Im Rahmen der Lizenzvereinbarung mit IBM müssen Sie die Anzahl der Trust Authority-Benutzer überwachen. Um Sie bei dieser Aufgabe zu unterstützen, stellt Trust Authority ein Tool zur Erstellung von Nutzungsberichten (Usage Report) zur Verfügung. Dieses Tool zeichnet die Anzahl der aktiven und inaktiven Benutzer im jeweiligen System auf sowie die Anzahl der aktiven und widerrufenen Zertifikate, die vom Trust Authority-CA seit der Installation des Produktes unterzeichnet worden sind. Es folgt eine Beschreibung der spezifischen Datenelemente des Nutzungsberichts (Usage Report):

Aktive Benutzer
: Benutzer mit mindestens einem aktiven Zertifikat, wobei *Benutzer* als Entität definiert ist, die über einen eindeutigen registrierten Namen (DN) verfügt.

Inaktive Benutzer
: Benutzer, die über keine aktiven Zertifikate verfügen, d. h. alle zuvor für diese Benutzer ausgestellten Zertifikate sind entweder abgelaufen oder wurden widerrufen.

Aktive Zertifikate
: Vom Trust Authority-CA unterzeichnete Zertifikate, die weder abgelaufen sind noch widerrufen wurden.

Widerrufene Zertifikate
: Zertifikate, die widerrufen wurden.

Vorgehensweise anhand von Programmsymbolen unter Windows NT

Wenn Sie Trust Authority auf einer Windows NT-Plattform ausführen und das Auswählen von Programmsymbolen gegenüber der Befehlseingabe in einem DOS-Befehlsfenster bevorzugen, können Sie anhand der folgenden Prozedur einen Nutzungsbericht (Usage Report) erstellen: Der Abschnitt „Beispielausgabe - Nutzungsbericht (Usage Report)" auf Seite 14 enthält ein Beispiel einer Berichtsausgabe.

1. Melden Sie sich als Trust Authority-Konfigurationsbenutzer an der Maschine an, auf der die Trust Authority-CA-Server-Komponente installiert ist. Der empfohlene Benutzername, der gleichzeitig auch der Standardbenutzername ist, lautet **cfguser**; möglicherweise wurde jedoch vom jeweiligen Unternehmen ein anderer Benutzername verwendet.
2. Wählen Sie nacheinander **Starten → Programme → IBM SecureWay Trust Authority → Trust Authority Usage Report** aus.

Befehlszeilenprozedur

Wenn Sie Trust Authority auf einer AIX-Plattform ausführen oder die Befehlseingabe gegenüber dem Auswählen von Programmsymbolen unter Windows NT bevorzugen, können Sie anhand der folgenden Prozedur einen Nutzungsbericht (Usage Report) erstellen: Der Abschnitt „Beispielausgabe - Nutzungsbericht (Usage Report)" auf Seite 14 enthält ein Beispiel einer Berichtsausgabe.

1. Melden Sie sich als Trust Authority-Konfigurationsbenutzer an der Maschine an, auf der die Trust Authority-CA-Server-Komponente installiert ist. Der empfohlene Benutzername, der gleichzeitig auch der Standardbenutzername ist, lautet **cfguser**. Wenn Sie Trust Authority unter Windows NT installiert haben, wurde vom jeweiligen Unternehmen möglicherweise ein anderer Benutzername verwendet.

2. Wechseln Sie in das Unterverzeichnis 'bin' des Trust Authority-Installationsverzeichnisses. In den folgenden Beispielen wird der Standardverzeichnispfad verwendet:
   - Unter AIX: `/usr/lpp/iau/bin`
   - Unter Windows NT: `c:\Program Files\IBM\Trust Authority\bin`
3. Geben Sie den folgenden Befehl ein:

   TAUsageReport

Beispielausgabe - Nutzungsbericht (Usage Report)

```
Trust Authority  Usage Report

Report generated on   :  Sep 28, 1999 16:10:20 EDT
    Total active users          =       42
    Total active certificates   =       53
    Total inactive users        =        6
    Total revoked certificates  =        3
```

Zertifikatsaktivität überwachen

Mit Hilfe des Trust Authority-Dienstprogramms 'Activity Report' können Sie Aktivitätsberichte erstellen, um die Anzahl der Zertifikate zu überwachen, die an einem bestimmten Tag oder innerhalb einer bestimmten Woche genehmigt, zurückgewiesen oder widerrufen wurden. Der Aktivitätsbericht (Activity Report) ist in zwei Teile untergliedert:

- Teil 1

  Im ersten Teil werden die Registratoren (RA-Administratoren) des jeweiligen Systems aufgeführt und die Zertifikatsaktivitäten der einzelnen Registratoren (Administratoren) aufgezeigt.

- Teil 2

  Im zweiten Teil des Berichts wird die Gesamtzahl der Zertifikate aufgeführt, die während des angeforderten Zeitraums genehmigt, zurückgewiesen oder widerrufen wurden. Dabei spielt es keine Rolle, ob diese Aktionen manuell durch einen Registrator oder automatisch über Regel-Exits ausgeführt wurden.

Vorgehensweise anhand von Programmsymbolen unter Windows NT

Wenn Sie Trust Authority auf einer Windows NT-Plattform ausführen und das Auswählen von Programmsymbolen gegenüber der Befehlseingabe in einem DOS-Befehlsfenster bevorzugen, können Sie anhand der folgenden Prozedur einen Aktivitätsbericht (Activity Report) erstellen: Der Abschnitt „Beispielausgabe - Aktivitätsbericht (Activity Report)" auf Seite 15 enthält ein Beispiel einer Berichtsausgabe.

1. Melden Sie sich als Trust Authority-Konfigurationsbenutzer an der Maschine an, auf der die Trust Authority-RA-Server-Komponente installiert ist. Der empfohlene Benutzername lautet **cfguser**; möglicherweise wurde jedoch vom jeweiligen Unternehmen ein anderer Benutzername verwendet.
2. Wählen Sie **Starten → Programme → IBM SecureWay Trust Authority → Trust Authority Activity Report** aus.
3. Wenn Sie vom System aufgefordert werden, die Berichtsart einzugeben, geben Sie **1** für einen wöchentlichen Bericht ein oder **2**, um eine Zusammenfassung der Aktivitäten anzuzeigen, die an einem bestimmten Tag stattfanden.
4. Wenn Sie zur Eingabe des Datums aufgefordert werden, geben Sie das Startdatum für die Woche ein, für die ein Bericht erstellt werden soll bzw. das exakte Datum für die Erstellung eines Tagesberichts. Geben Sie das Datum im Format jjjj-mm-tt ein, beispielsweise 1999-10-01.

Befehlszeilenprozedur

Wenn Sie Trust Authority auf einer AIX-Plattform ausführen oder die Befehlseingabe gegenüber dem Auswählen von Programmsymbolen unter Windows NT bevorzugen, können Sie anhand der folgenden Prozedur einen Aktivitätsbericht (Activity Report) erstellen: Der Abschnitt „Beispielausgabe - Aktivitätsbericht (Activity Report)" enthält ein Beispiel einer Berichtsausgabe.

1. Melden Sie sich als Trust Authority-Konfigurationsbenutzer an der Maschine an, auf der die Trust Authority-RA-Server-Komponente installiert ist. Der empfohlene Benutzername, der gleichzeitig auch der Standardbenutzername ist, lautet **cfguser**. Wenn Sie Trust Authority unter Windows NT installiert haben, wurde vom jeweiligen Unternehmen möglicherweise ein anderer Benutzername verwendet.
2. Wechseln Sie in das Unterverzeichnis 'bin' des Trust Authority-Installationsverzeichnisses. In den folgenden Beispielen wird der Standardverzeichnispfad verwendet:
   - Unter AIX: `/usr/lpp/iau/bin`
   - Unter Windows NT: `c:\Program Files\IBM\Trust Authority\bin`
3. Geben Sie den folgenden Befehl ein:

   TAActivityReport
4. Wenn Sie vom System aufgefordert werden, die Berichtsart einzugeben, geben Sie **1** für einen wöchentlichen Bericht ein oder **2**, um eine Zusammenfassung der Aktivitäten anzuzeigen, die an einem bestimmten Tag stattfanden.
5. Wenn Sie zur Eingabe des Datums aufgefordert werden, geben Sie das Startdatum für die Woche ein, für die ein Bericht erstellt werden soll bzw. das exakte Datum für die Erstellung eines Tagesberichts. Geben Sie das Datum im Format jjjj-mm-tt ein, beispielsweise 1999-10-01.

Anmerkung: Um die Eingabeaufforderungen zu umgehen, können Sie die folgenden Befehlsparameter in der Befehlszeile angeben:

```
TAActivityReport
[-t reportType(1/2)] [-d startDate(jjjj-mm-tt)]
```

Beispiel: **TAActivityReport -t 2 -d 1999-09-27**

Beispielausgabe - Aktivitätsbericht (Activity Report)

Im folgenden Beispiel wird ein täglicher Aktivitätsbericht dargestellt. Der wöchentliche Bericht ist entsprechend aufgebaut, enthält jedoch eine Zusammenfassung der wöchentlichen Summen der jeweiligen Aktivitäten.

```
Trust Authority Activity Report
Report generated on         : Sep 28, 1999 15:59:23 EDT
Date of daily report        : 1999-09-27
Daily Activity Report for RA Administrators

  RA Administrator DN                  Approved          Rejected          Revoked
  CN=RAadmin1, OU=PKI, O=IBM, C=US           23                 6                1
  CN=RAadmin2, OU=PKI, O=IBM, C=US           14                 2                0
  CN=RAadmin3, OU=PKI, O=IBM, C=US           55                 8                4

Daily Activity Report for the System
  Approved    =      92
  Rejected    =      16
  Revoked     =       5
```

WebSphere Application Server verwalten

IBM WebSphere besteht aus einer Gruppe von Softwareprodukten, mit denen Unternehmen leistungsfähige Web-Sites entwickeln und verwalten können. Der WebSphere Application Server stellt zusammen mit dem IBM HTTP Server in Trust Authority die Infrastruktur für Web-Server-Funktionalität bereit.

Status des WebSphere Application Server prüfen

Je nach Umgebung können Sie den Status des WebSphere Application Server mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Root an.
  2. Prüfen Sie die Prozeßtabelle und suchen Sie nach folgender Zeichenfolge:

     ```
     OutofProcEngine
     ```

     Finden Sie diesen Prozeß, fahren Sie mit Schritt 3 fort. Finden Sie diesen Prozeß nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung" auf Seite 120 nach.
  3. Informationen zum Zugriff auf die WebSphere-Verwaltungsseiten und zur Ermittlung des Server-Status finden Sie in der WebSphere-Dokumentation.
- Unter Windows NT:
  1. Melden Sie sich bei Windows NT als Systemadministrator an.
  2. Starten Sie den Task-Manager durch Drücken der Tastenkombination **Strg Alt** und **Entf**.
  3. Wählen Sie die Registerkarte **Prozesse** aus.
  4. Suchen Sie nach mindestens einem Vorkommen des Prozesses java.exe.

     Finden Sie diesen Prozeß, fahren Sie mit Schritt 5 fort. Finden Sie diesen Prozeß nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung" auf Seite 120 nach.
  5. Informationen zum Zugriff auf die WebSphere-Verwaltungsseiten und zur Ermittlung des Server-Status finden Sie in der WebSphere-Dokumentation.

WebSphere Application Server-Protokolle prüfen

Sie können die Protokolle prüfen, in denen die Transaktionen zwischen dem WebSphere Application Server und dem IBM Trust Authority Setup Wizard aufgezeichnet werden. Die Positionen dieser Protokolle werden im Abschnitt Tabelle 2 beschrieben.

Tabelle 2. WebSphere Application Server-Protokolle über Transaktionen mit dem Setup Wizard

AIX-Standardpfad	Windows NT-Standardpfad	Anmerkungen
/usr/lpp/iau/etc/logs/jvm_stderr.log	c:\Program Files\IBM\Trust Authority\etc\logs\jvm_stderr.log	Der Standardpfad für Fehlernachrichten der Java Virtual Machine (JVM).
/usr/lpp/iau/etc/logs/jvm_stdout.log	c:\Program Files\IBM\Trust Authority\etc\logs\jvm_stdout.log	Der Standardausgabepfad der JVM.

Sie können die Protokolle prüfen, die die Transaktionen zwischen dem IBM WebSphere Application Server und Ihrer Registrierungsanwendung aufzeichnen. Die Positionen dieser Protokolle werden in Tabelle 3 erläutert.

Tabelle 3. IBM WebSphere Application Server - Protokolle über Transaktionen mit der Registrierungsanwendung

AIX-Standardpfad	Windows NT-Standardpfad	Anmerkungen
/usr/lpp/iau/pkrf/Domains/YourDomain /etc/logs/jvm_stderr.log	c:\Program Files\IBM\Trust Authority\pkrf\Domains\YourDomain\ etc\logs\jvm_stderr.log	Der Standardpfad für Fehlernachrichten der Java Virtual Machine (JVM).
/usr/lpp/iau/pkrf/Domains/YourDomain /etc/logs/jvm_stdout.log	c:\Program Files\IBM\Trust Authority\pkrf\Domains\YourDomain\n\ etc\logs\jvm_stdout.log	Der Standardausgabe-pfad der JVM.
/usr/lpp/iau/pkrf/Domains/ YourDomain/logs/*hostname_ssl-port* -ssl-error.log	c:\Program Files\IBM\Trust Authority\pkrf\Domains\YourDomain\ logs*hostname_ssl-port* -ssl-error.log	Fehlernachrichten von Transaktionen über sichere HTTP-Verbindungen. Zwei Arten sind möglich: Vom Client authentifizierte und nicht vom Client authentifizierte Transaktionen.
/usr/lpp/iau/pkrf/Domains/YourDomain/ logs/*hostname*error.log	c:\Program Files\IBM\Trust Authority\pkrf\Domains\YourDomain\ logs*hostname_public-port*error.log	Fehlernachrichten von Transaktionen über öffentliche HTTP-Verbindungen.

HTTP Server verwalten

IBM HTTP Server ist das Web-Server-Produkt, das die web-gestützte Kommunikation mit Browsern und anderen Programmen verwaltet. Der HTTP-Dämon (HTTPD) ist die Hauptkomponente des Web-Servers. Trust Authority verwendet mehrere HTTP-Dämonen. Diese HTTP-Dämonexemplare verwalten öffentliche, verschlüsselte sowie vom Client authentifizierte und verschlüsselte Verbindungen. Detaillierte Informationen zu Web-Servern und zu den verschiedenen Verbindungsarten, die in Trust Authority zur Verwaltung unterschiedlicher Transaktionen eingesetzt werden, finden Sie im Abschnitt „Web-Server" auf Seite 74.

Status des HTTP Server prüfen

Je nach Umgebung können Sie den Status des HTTP Server mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Root an.
  2. Prüfen Sie die Prozeßtabelle und suchen Sie nach folgender Zeichenfolge:
     - `sidd` (einmal)
     - `httpd` (mindestens zweimal)

     Sind diese drei Prozesse vorhanden, fahren Sie mit Schritt 3 auf Seite 18 fort. Sind nicht alle dieser drei Prozesse vorhanden, lesen Sie bitte im Abschnitt „Fehlerbehebung" auf Seite 120 nach.

3. Wechseln Sie in das Verzeichnis bin. Dieses Verzeichnis hat folgenden Standardpfad:

   ```
   /usr/lpp/iau/bin
   ```

4. Prüfen Sie die Anschlüsse, indem Sie für jeden Anschluß folgenden Befehl eingeben:

   checkSrvPortStatus -p *Port* **-s** *Server* **-r1 -w1**

   Hierbei steht *Port* für die Nummer des zu prüfenden Anschlusses und *Server* für den Namen des zugeordneten HTTP Servers. Eine Übersicht der standardmäßigen HTTP Server- und Anschluß-Konfigurationen von Trust Authority finden Sie im Abschnitt Tabelle 13 auf Seite 75.

   Ist die Antwort des geprüften Anschlusses erfolgreich, wird folgende Nachricht angezeigt:

   Port:*Port* on *Server* is bound.

   Hierbei steht *Port* für den geprüften Anschluß und *Server* für den Namen des entsprechenden Servers.

- Unter Windows NT:
  1. Melden Sie sich bei Windows NT als Systemadministrator an.
  2. Starten Sie den Task-Manager durch Drücken der Tastenkombination **Strg**, **Alt** und **Entf**.
  3. Wählen Sie die Registerkarte **Prozesse** aus.
  4. Suchen Sie nach zwei Exemplaren des Prozesses Apache.exe.

     Sind diese zwei Prozesse vorhanden, fahren Sie mit Schritt 5 fort. Sind diese beiden Prozesse nicht vorhanden, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 120 nach.
  5. Wechseln Sie an der MS DOS-Eingabeaufforderung in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:

     ```
     c:\Program Files\IBM\Trust Authority\bin
     ```

  6. Prüfen Sie die Anschlüsse, indem Sie für jeden Anschluß folgenden Befehl eingeben:

     checkSrvPortStatus -p *Port* **-s** *Server* **-r1 -w1**

     Hierbei steht *Port* für die Nummer des zu prüfenden Anschlusses und *Server* für den Namen des zugeordneten HTTP Servers. Eine Übersicht der standardmäßigen HTTP Server- und Anschluß-Konfigurationen von Trust Authority finden Sie im Abschnitt Tabelle 13 auf Seite 75.

     Ist die Antwort des geprüften Anschlusses erfolgreich, wird folgende Nachricht angezeigt:

     Port:*Port* on *Server* is bound.

     Hierbei steht *Port* für den geprüften Anschluß und *Server* für den Namen des entsprechenden Servers.

HTTP Server-Protokolle prüfen

Sie können die Protokolle prüfen, die Transaktionen zwischen dem IBM HTTP Server und dem Trust Authority Setup Wizard aufzeichnen. Die Positionen dieser Protokolle werden im Abschnitt Tabelle 4 erläutert.

Tabelle 4. HTTP Server-Protokolle über Transaktionen mit dem Setup Wizard

AIX-Standardpfad	Windows NT-Standardpfad	Anmerkungen
/usr/lpp/iau/logs/oop_native.log.ERROR	c:\Program Files\IBM\Trust Authority\logs\oop_native.log.ERROR	Fehlernachrichten aus dem ursprünglichen Codeabschnitt der inaktiven Maschine.
/usr/lpp/iau/logs/ oop_native.log.INFORM	c:\Program Files\IBM\Trust Authority\logs\ oop_native.log.INFORM	Informationsnachrichten aus dem ursprünglichen Codeabschnitt der inaktiven Maschine.
/usr/lpp/iau/logs/ oop_native.log.WARNING	c:\Program Files\IBM\Trust Authority\logs\ oop_native.log.WARNING	Warnungen aus dem ursprünglichen Codeabschnitt der inaktiven Maschine.

Sie können die Protokolle prüfen, die Transaktionen zwischen dem IBM HTTP Server und Ihrer Registrierungsanwendung aufzeichnen. Die Positionen dieser Protokolle werden im Abschnitt Tabelle 5 erläutert.

Tabelle 5. HTTP Server-Protokolle über Transaktionen mit Ihrer Registrierungsanwendung

AIX-Standardpfad	Windows NT-Standardpfad	Anmerkungen
usr/lpp/iau/pkrf/Domain/YourDomain/ logs/apache.log.ERROR.PID	c:\Program Files\IBM\Trust Authority\Domains\YourDomain\logs\ apache.log.ERROR.PID	Fehlernachrichten des IBM HTTP Server.
usr/lpp/iau/pkrf/Domain/YourDomain/ logs/apache.log.INFORM.PID	c:\Program Files\IBM\Trust Authority\Domains\YourDomain\logs\ apache.log.INFORM.PID	Informationsnachrichten des IBM HTTP Server.
usr/lpp/iau/pkrf/Domain/YourDomain/ logs/apache.log.TRACE.PID	c:\Program Files\IBM\Trust Authority\Domains\YourDomain\logs\ apache.log.TRACE.PID	Das Trace-Protokoll des IBM HTTP Server.

CA-Server verwalten

In diesem Abschnitt werden Prozeduren für Betrieb und Verwaltung des Trust Authority Zertifikatsaussteller-Servers (CA-Server) erläutert. Der CA-Server verwaltet die server-seitigen Tasks für den Trust Authority-CA. Er befindet sich zusammen mit seinem DB2-Datenbankexemplar auf einer lokalen oder fernen Maschine.

Zur Verwaltung des CA-Servers müssen Sie in der Regel die nachfolgend beschriebenen Tasks ausführen.

- Verwenden Sie den Editor IniEditor, um folgende Änderungen an der Konfigurationsdatei jonahca.ini vorzunehmen:
  - Ändern Sie den vom CA überwachten TCP-Anschluß.
  - Ändern Sie das Sendeaufrufintervall für PKIX-Nachrichten.
  - Ändern Sie die CRL-Einstellungen.
  - Ändern Sie die ICL-Schutzregel.
- Ändern Sie den ICL-Schutzschlüssel.
- Prüfen Sie die Integrität der CA-Server-Datenbank.
- Verwenden Sie das Dienstprogramm CA Certification für gegenseitige Zertifizierungen und CA-Hierarchien.
- Prüfen Sie die Protokolle des CA-Servers.
- Prüfen Sie den Status des CA-Servers.
- Aktivieren Sie die CRL-Verteilungspunkte.

Vom CA-Server überwachten Anschluß ändern

Der vom CA-Server überwachte Anschluß ist der Anschluß, der vom CA auf PKIX-Nachrichten geprüft wird. Gehen Sie wie folgt vor, um den Wert für diesen Anschluß zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor, und laden Sie die Konfigurationsdatei jonahca.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **Transport** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **TCPPort** aus.
5. Ändern Sie im angezeigten Editierfeld die Anschlußnummer.
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie IniEditor erneut und laden Sie die Konfigurationsdatei jonahra.ini. (Diese Datei kann sich je nach Installation auf einer lokalen oder einer fernen Maschine befinden).
8. Wählen Sie den Abschnitt **URLs** aus.
9. Ändern Sie im angezeigten Editierfeld die Anschlußnummer.
10. Wählen Sie den Abschnitt **General** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **Issuer1URL1** aus.
11. Ändern Sie im angezeigten Editierfeld die Anschlußnummer.
12. Speichern Sie die Datei und beenden Sie das Programm.
13. Starten Sie das Trust Authority-System.

CA-Sendeaufrufintervall ändern

Das CA-Sendeaufrufintervall ist die Zeit in Sekunden (s), Minuten (m) oder Stunden (h) zwischen den Abfragen der Arbeitsablaufwarteschlange durch den CA-Server. Die Elemente in dieser Warteschlange, deren Zuteilungszeit abgelaufen ist, werden für die Verarbeitung zugeteilt. Gehen Sie wie folgt vor, um das Sendeaufrufintervall zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor, und laden Sie die Konfigurationsdatei jonahca.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **Transport** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **PollInterval** aus.
5. Ändern Sie im angezeigten Editierfeld den Wert für das Sendeaufrufintervall.
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie das Trust Authority-System.

CRL-Einstellungen ändern

Eine Zertifikatswiderrufsliste (CRL) ist eine digital unterzeichnete, mit Zeitmarken versehene Liste der Zertifikate, die vom Zertifikatsaussteller (CA) widerrufen wurden. In der Konfigurationsdatei des CA-Servers können folgende Werte geändert werden, um die Art der CRL-Verwaltung zu beeinflussen:

- Die Zeit zwischen den geplanten CRL-Erstellungen
- Die Gültigkeitsdauer einer CRL

Zeit zwischen CRL-Erstellungen ändern

Gehen Sie wie folgt vor, um die Regeln für Zertifikate und die gegenseitige Zertifizierung bezüglich der Intervalle zwischen geplanten Veröffentlichungen einer CRL zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor, und laden Sie die Konfigurationsdatei jonahca.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **CertPolicy** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **TimeBetweenCRLs** aus.
5. Ändern Sie im angezeigten Editierfeld die Zeit zwischen den Erstellungen neuer CRLs.

   Der Wert wird als Intervall in Minuten (m), Stunden (h) oder Tagen (d) angegeben. Beispiel: `1d`. Der Wert muß kleiner sein als der Wert für die Gültigkeitsdauer der CRL.
6. Wählen Sie den Abschnitt **CrossCertPolicy** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **TimeBetweenCRLs** aus.
7. Ändern Sie im angezeigten Editierfeld die Zeit zwischen den Erstellungen neuer CRLs.

   Der Wert wird als Intervall in Minuten (m), Stunden (h) oder Tagen (d) angegeben. Beispiel: `1d`. Der Wert muß kleiner sein als der Wert für die Gültigkeitsdauer der CRL.
8. Speichern Sie die Datei und beenden Sie das Programm.
9. Starten Sie das Trust Authority-System.

Gültigkeitsdauer einer CRL ändern

Gehen Sie wie folgt vor, um die Regeln für Zertifikate und die gegenseitige Zertifizierung bezüglich der Gültigkeitsdauer einer CRL zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor, und laden Sie die Konfigurationsdatei jonahca.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **CertPolicy** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **CRLDuration** aus.

5. Ändern Sie im angezeigten Editierfeld die Zeit, für die eine CRL gültig ist. Der Wert wird als Intervall in Minuten (m), Stunden (h) oder Tagen (d) angegeben. Beispiel: `2d`.
6. Wählen Sie den Abschnitt **CrossCertPolicy**, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **CRLDuration** aus.
7. Ändern Sie im angezeigten Editierfeld die Zeit, für die eine CRL gültig ist. Der Wert wird als Intervall in Stunden, Minuten oder Tagen angegeben. Beispiel: `2d`.
8. Speichern Sie die Datei und beenden Sie das Programm.
9. Starten Sie das Trust Authority-System.

ICL-Schutzregel ändern

Die Liste der ausgestellten Zertifikate (Issued Certificates List, ICL) enthält die ausgestellten Zertifikate zusammen mit ihrem jeweiligen Status. Beim ICL-Schutzschlüssel handelt es sich um einen chiffrierten Schlüssel, der im Trust Authority-Schlüsselspeicher (KeyStore) gespeichert ist und verwendet wird, um für alle Spalten der ICL Werte für Nachrichtenauthentifizierungscodes (MAC) zu berechnen. Wenn der berechnete MAC-Wert nicht mit dem gespeicherten MAC-Wert übereinstimmt, verwendet das System die ICL-Schutzregel und führt entsprechende Aktionen aus.

Um die ICL-Schutzregel zu ändern, gehen Sie folgendermaßen vor:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor, und laden Sie die Konfigurationsdatei jonahca.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **ICL** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **IclProtectionPolicy** aus.
5. Ändern Sie im angezeigten Editierfeld den Wert der ICL-Schutzregel in einen Wert, der den Bedürfnissen Ihres Unternehmens gerecht wird. Folgende Werte sind zulässig:
   - Ignore — Das System ignoriert die Abweichung und zeigt keine Nachrichten an.

     Anmerkung: Dieser Wert wirkt sich auf den Betrieb des Tools für die CA-Integritätsprüfung aus (siehe „Integrität der CA-Server-Datenbank prüfen" auf Seite 24). Wenn Sie *Ignore* angeben, kann das Tool zur CA-Integritätsprüfung keinen Mißbrauch ermitteln, selbst wenn ein solcher existiert.
   - ContinueWithMessage — Das System zeigt eine Warnung an, setzt die Transaktion jedoch fort.
   - TerminateTransaction — Das System zeigt eine Fehlernachricht an und beendet die Transaktion.
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie das Trust Authority-System.

ICL-Schutzschlüssel ändern

Der ICL-Schutzschlüssel wird niemals Benutzern oder Administratoren preisgegeben. Um jedoch einem Mißbrauch oder einer unbeabsichtigten Dateninkonsistenz vorzubeugen, empfiehlt es sich, den ICL-Schutzschlüssel in regelmäßigen Abständen zu ändern. Trust Authority stellt das Befehlszeilen-Tool 'CARemac' zur Verfügung, mit dem ein neuer ICL-Schutzschlüssel zur Berechnung eines neuen MAC-Wertes generiert wird. Um den ICL-Schutzschlüssel zu ändern, gehen Sie folgendermaßen vor:

1. Wechseln Sie zu der Maschine, auf der der CA-Server installiert ist.
2. Stoppen Sie das Trust Authority-System mit Hilfe der unter „Server-Komponenten starten und stoppen" auf Seite 7 beschriebenen Prozedur.
3. Führen Sie das Tool für den ICL-Schutzschlüssel aus, indem Sie in der Trust Authority-Befehlszeile den Befehl CARemac (der den entsprechenden Trust Authority-Installationspfad enthält) eingeben. Beispiel:
   - Unter AIX, wenn Sie den Standardinstallationspfad von Trust Authority verwenden:

     ```
     CARemac in /usr/lpp/iau/bin
     ```

   - Unter Windows NT, wenn Sie den Standardinstallationspfad von Trust Authority verwenden:

     ```
     CARemac in "c:Program Files\IBM\Trust Authority\bin"
     ```

   Das Tool fordert Sie zur Eingabe des Kennworts für das Trust Authority-Steuerprogramm auf.
4. Geben Sie das Kennwort für das Trust Authority-Steuerprogramm ein.
5. Starten Sie das Trust Authority-System mit Hilfe der unter „Server-Komponenten starten und stoppen" auf Seite 7 beschriebenen Prozedur.

Integrität der CA-Server-Datenbank prüfen

Trust Authority stellt das Tool 'CAIntegrityCheck' zur Verfügung, mit dessen Hilfe Mißbräuche der CA-Server-Datenbank ermittelt werden können. Unter normalen Umständen führt der CA Schutzprüfungen nur für den Teilsatz der ICL-Einträge aus, auf den zu einem bestimmten Zeitpunkt gerade zugegriffen wird. Mit anderen Worten: Der CA prüft lediglich diejenigen Einträge, die bei Erstellung der CRL ausgewählt sind, demnach also den Status *revoked* (widerrufen) haben. Daher werden die meisten der ICL-Einträge während des normalen Trust Authority-CA-Betriebs nicht auf ihre Integrität hin geprüft.

Wenn Sie die Integrität der gesamten CA-Datenbank prüfen wollen, müssen Sie das Tool zur CA-Integritätsprüfung verwenden. Dieses ausführbare Programm liest alle Einträge in der ICL und führt für sie entsprechende Integritätsprüfungen durch. Das Programm ändert zwar nicht den Schutzschlüssel, doch ist es dennoch erforderlich, den CA während der Ausführung des Programms herunterzufahren.

Um die Integrität der CA-Server-Datenbank zu prüfen, gehen Sie folgendermaßen vor:

1. Wechseln Sie zu der Maschine, auf der der CA-Server installiert ist.
2. Stoppen Sie das Trust Authority-System mit Hilfe der unter „Server-Komponenten starten und stoppen" auf Seite 7 beschriebenen Prozedur.
3. Führen Sie das Tool zur Prüfung der Integrität der CA-Datenbank aus, indem Sie in der Trust Authority-Befehlszeile folgenden Befehl eingeben (der den entsprechenden Trust Authority-Installationspfad enthält). Beispiel:

- Unter AIX, wenn Sie den Standardinstallationspfad von Trust Authority verwenden:

  ```
  CAIntegrityCheck in /usr/lpp/iau/bin
  ```

- Unter Windows NT, wenn Sie den Standardinstallationspfad von Trust Authority verwenden:

  ```
  CAIntegrityCheck in "c:Program Files\IBM\Trust Authority\bin"
  ```

Das Tool fordert Sie zur Eingabe des Kennworts für das Trust Authority-Steuerprogramm auf.

4. Geben Sie das Kennwort für das Trust Authority-Steuerprogramm ein.
5. Starten Sie das Trust Authority-System mit Hilfe der unter „Server-Komponenten starten und stoppen" auf Seite 7 beschriebenen Prozedur.

CA-Zertifikat mit Hilfe gegenseitiger Zertifizierung anfordern

Sie können im Namen des Trust Authority-CA ein CA-Zertifikat von einem anderen CA anfordern, wenn Sie das Sicherungsmodell für die gegenseitige Zertifizierung verwenden. Die gegenseitige Zertifizierung ermöglicht es zuverlässigen CAs, die Anerkennung gegenseitig ausgestellter Zertifikate als Identitätsnachweis zu vereinbaren. Obwohl die gegenseitige Zertifizierung zwischen CAs in beiden Richtungen erfolgen kann, werden in Trust Authority Anforderungen für die gegenseitige Zertifizierung nur in einer Richtung unterstützt.

Anmerkung: Trust Authority unterstützt eine gegenseitige Zertifizierung nur zwischen CAs, die das PKIX-Zertifikatsverwaltungsprotokoll (Certificate Management Protocol, CMP) einhalten.

Verwenden Sie für die gegenseitige Zertifizierung mit einem anderen CA das Trust Authority-Dienstprogramm CA Certification. Dieses Dienstprogramm ist ein Befehlszeilen-Tool. Beim Starten können Sie Optionen für die Standardzertifikatserweiterung für Namenseinschränkungen definieren. Ein kleingeschriebener Buchstabe steht für die Aufnahme in die Liste zulässiger Unterverzeichnisstrukturen. Ein großgeschriebener Buchstabe steht für die Aufnahme in die Liste nicht zulässiger Unterverzeichnisstrukturen. In der Regel werden nicht zulässige Unterverzeichnisstrukturen nur für einen Adreßtyp angegeben, für den auch eine Liste zulässiger Unterverzeichnisstrukturen existiert.

Die nachfolgenden Abschnitte erläutern anhand von Beispielen die Schritte, die zum Erhalt eines CA-Zertifikats mit Hilfe der gegenseitigen Zertifizierung erforderlich sind.

Erforderliche Schritte für die gegenseitige Zertifizierung

Befolgen Sie die nachfolgend beschriebenen Anweisungen, um ein CA-Zertifikat mit Hilfe der gegenseitigen Zertifizierung anzufordern.

1. Führen Sie im Namen des anfordernden CA folgende Schritte gemäß den Anweisungen zur web-gestützten Registrierung im *Benutzerhandbuch* aus:
   a. Führen Sie eine Vorabregistrierung aus und geben Sie an, daß die Anforderung für einen CA erfolgt.

      Achten Sie beim Ausfüllen des Registrierungsformulars darauf, einen registrierten Namen (DN) einzugeben, der mit dem des anfordernden CA übereinstimmt.
   b. Prüfen Sie den Status der Registrierungsanforderung.
   c. Befolgen Sie die Anweisung am Ende des Abschnitts, um die Vorabregistrierungsdatei zu speichern.

2. Übertragen Sie die Vorabregistrierungsdatei auf die Maschine, auf der sich der anfordernde CA befindet.
3. Melden Sie sich bei Trust Authority als der Benutzer an, der das System auf der Maschine installiert hat, auf der sich der anfordernde CA befindet.
4. Führen Sie den Befehl CaCertRq aus, und zwar unter AIX über die Befehlszeile und unter Windows NT über die DOS-Eingabeaufforderung.

   Stellen Sie bei Ausführung des Befehls CaCertRq sicher, daß Sie den absoluten Pfad und den Namen der Vorabregistrierungsdatei eingeben. Informationen zur Befehlssyntax und Parameterbeschreibungen finden Sie im Abschnitt „Dienstprogramm CA Certification" auf Seite 103.

   Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (" ") setzen. Für den Befehl 'CaCertRq' beispielsweise würden Sie den Parameter -r *vorabregistrierungspfad* (mit eingebetteten Leerzeichen) folgendermaßen angeben:

   ```
   CaCertRq -d .companyA.com -r "c:\Program Files\IBM\Trust
        Auhority\ccprereg.reg" -P 1835 -W Secure99
   ```

IP-Adreßmaske angeben

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die Gültigkeit des Zertifikats auf die IP-Adressen einschränkt, die von Ihrem Unternehmen verwendet werden.

Im folgenden Beispiel ist das Betriebssystem AIX, Ihr Unternehmen verwendet IP-Adressen im Bereich von 9.0.0.0. bis 9.255.255.254, die Vorabregistrierungsdatei befindet sich im Pfad /tmp/ccprereg.reg, und das Kennwort lautet Secure99. Folgender Befehl plaziert den angegebenen Adressenbereich in der Liste zulässiger Unterverzeichnisstrukturen:

```
CaCertRq -i 9.0.0.0/255.0.0.0 -r /tmp/ccprereg.reg -P 1835 -W Secure99
```

DNS-Adressen angeben

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die Gültigkeit des Zertifikats auf eine Gruppe von DNS-Adressen einschränkt.

Im folgenden Beispiel wird das Betriebssystem Windows NT verwendet, und alle Trust Authority-CA-Hosts verfügen über DNS-Adressen mit der Endung ".companyA.com". Mit folgendem Befehl werden die angegebenen DNS-Adressen in der Liste der zulässigen Unterverzeichnisstrukturen plaziert:

```
CaCertRq -d .companyA.com -r c:\temp\ccprereg.reg -P 1835 -W Secure99
```

Anmerkung: Beginnt eine DNS-Adresse mit einem Punkt, werden alle Hosts einbezogen, die mit dieser Unterzeichenfolge (einschließlich ".") enden. Diese Adressen werden in die Liste der Unterverzeichnisstrukturen aufgenommen. Beginnt die Adresse nicht mit einem Punkt, wird nur der Host einbezogen, dessen Name der Zeichenfolge entspricht.

Der Einschränkung ″.companyA.com″ entsprechen beispielsweise us.companyA.com, vnet.companyA.com und w3.software.companyA.com, jedoch nicht companyA.com (oder kidcompanyA.com) selbst. Der Einschränkung companyA.com entsprechen companyA.com, jedoch nicht us.companyA.com oder die übrigen Adressen. Daraus folgt, daß eine zulässige Unterverzeichnisstrukturen ohne führenden Punkt ″.″ nur einen möglichen Knoten angibt. Angaben ohne einen führenden Punkt werden primär für nicht zulässige Unterverzeichnisstrukturen verwendet.

E-Mail-Adressen angeben

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die Gültigkeit des Zertifikats auf eine Gruppe von E-Mail-Adressen einschränkt.

Im folgenden Beispiel wird das Betriebssystem Windows NT verwendet, alle Trust Authority-CA-Hosts verfügen über E-Mail-Adressen, die mit .us.companyA.com enden, Pfad und Dateiname der Vorabregistrierungsdatei lauten a:\ccprereg.reg, und das Kennwort lautet Secure99. Folgender Befehl plaziert die angegebenen E-Mail-Adressen in der Liste zulässiger Unterverzeichnisstrukturen:

```
CaCertRq -m .us.companyA.com -r a:\ccprereg.reg -P 1835 -W Secure99
```

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die Gültigkeit des Zertifikats auf alle bis auf ein Element einer Gruppe von E-Mail-Adressen einschränkt.

Im folgenden Beispiel wird das Betriebssystem Windows NT verwendet, der Trust Authority-CA-Host hat die E-Mail-Adresse outCA.us.companyA.com, Pfad und Dateiname der Vorabregistrierungsdatei lauten a:\ccprereg.reg, und das Kennwort lautet Secure99. Folgender Befehl plaziert die angegebenen E-Mail-Adressen in der Liste nicht zulässiger Unterverzeichnisstrukturen:

```
CaCertRq -m .us.companyA.com -M outCA.us.companyA.com -r a:\ccprereg.reg -P 1835
   -W Secure99
```

URIs angeben

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die Gültigkeit des Zertifikats auf eine Gruppe von URIs (Uniform Resource Identifiers, eine Kennungskategorie, die hauptsächlich aus URL-Adressen besteht) einschränkt.

Im folgenden Beispiel wird das Betriebssystem AIX verwendet, alle Trust Authority-CA-Hosts verfügen über Namen, die mit .xyz.com enden, Pfad und Dateiname der Vorabregistrierungsdatei lauten /tmp/ccprereg.reg, und das Kennwort lautet Secure99. Folgender Befehl plaziert die angegebene URI in der Liste zulässiger Unterverzeichnisstrukturen:

```
CaCertRq -u .xyz.com -r /tmp/ccprereg.reg -P 1835 -W Secure99
```

Anmerkung: Der Knotenabschnitt (in einer Baumstruktur ein Punkt, an dem untergeordnete Datenelemente ihren Ursprung haben) der URI unterliegt den im Abschnitt „DNS-Adressen angeben” auf Seite 26 beschriebenen Regeln, sofern er keine IP-Adressen enthält. In diesem Fall wird er als exakte Übereinstimmung behandelt.

Verzeichniseinträge angeben

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die Gültigkeit des Zertifikats auf eine Gruppe von Verzeichniseinträgen mit den gleichen RDNs (Relative Distinguished Names) einschränkt.

Im folgenden Beispiel wird das Betriebssystem AIX verwendet, alle Trust Authority-CA-Hosts verfügen über RDNs, die den angegebenen RDNs (/C=US/O=companyA/OU=departmentB) entsprechen, Pfad und Dateiname der Vorabregistrierungsdatei lauten /tmp/ccprereg.reg, und das Kennwort lautet Secure99. Folgender Befehl plaziert den angegebenen RDN in der Liste der zulässigen Unterverzeichnisstrukturen:

```
CaCertRq -n "/C=US/O=companyA/OU=departmentB" -r /tmp/ccprereg.reg -P 1835
   -W Secure99
```

CA-Zertifikat mit Hilfe des Hierarchiemodells anfordern

Sie können ein CA-Zertifikat mit Hilfe des Hierarchiemodells von einem anderen CA anfordern. Sie können dies beispielsweise tun, wenn Trust Authority an mehreren Orten installiert ist und Sie eine zuverlässige CA-Hierarchie etablieren wollen. CAs betrachten die CAs als zuverlässig, die in der Hierarchie über ihnen stehen, und akzeptieren deren Zertifikate als Identitätsnachweis.

Anmerkung: Trust Authority unterstützt eine hierarchische Zertifizierung nur zwischen CAs, die das PKIX-Zertifikatsverwaltungsprotokoll (Certificate Management Protocol, CMP) sowie die Protokolle PKCS #7 und PKCS #10 einhalten.

Nutzen Sie das Trust Authority-Befehlszeilendienstprogramm CA Certification, um eine CA-Hierarchie zu definieren. Wenn Sie dieses Tool starten, müssen Sie mindestens eine Option für die Standardzertifikatserweiterung für Namenseinschränkungen definieren. (Detaillierte Beschreibungen der Zertifikatserweiterungen finden Sie im Abschnitt „Zertifikatserweiterungen" auf Seite 64.) Ein kleingeschriebener Buchstabe steht für die Aufnahme in die Liste zulässiger Unterverzeichnisstrukturen. Ein großgeschriebener Buchstabe steht für die Aufnahme in die Liste nicht zulässiger Unterverzeichnisstrukturen. In der Regel werden nicht zulässige Unterverzeichnisstrukturen nur für einen Adreßtyp angegeben, für den auch eine Liste zulässiger Unterverzeichnisstrukturen existiert.

Anmerkung: Wenn Sie planen, als Teil Ihrer allgemeinen Hierarchielösung die hierarchischen CA-Zertifikate in Netscape Communicator herunterzuladen, sollten Sie die Markierung ″-m ..″ mit dem Dienstprogramm CA Certification verwenden, um die Erweiterung für Namenseinschränkungen (Name Constraints) aus dem resultierenden CA-Zertifikat auszuschließen. Mit Ausnahme von ″-m ..″ sollten Sie keine anderen der Befehlszeilenoptionen für Namenseinschränkungen (also nicht -i/I, -d/D, -u/U, -n/N oder -m/-M) mit dem Dienstprogramm CA Certification verwenden. Die Syntax für einen solchen Befehl sieht folgendermaßen aus:

```
CaCertRq -m .. -h -r
vorabregistrierungspfad
-P 1835 -W kennwort
```

Die nachfolgenden Abschnitte erläutern anhand von Beispielen die Schritte, die zum Erhalt eines CA-Zertifikats mit Hilfe des Hierarchiemodells erforderlich sind.

Schritte zur Anforderung eines CA-Zertifikats mit Hilfe des Hierarchiemodells

Befolgen Sie die nachfolgend beschriebenen Anweisungen, um ein CA-Zertifikat mit Hilfe des Hierarchiemodells anzufordern:

1. Führen Sie im Namen des anfordernden CA folgende Schritte gemäß den Anweisungen zur web-gestützten Registrierung im *Benutzerhandbuch* aus:
   a. Führen Sie eine Vorabregistrierung aus und geben Sie an, daß die Anforderung für einen CA erfolgt.

      Achten Sie beim Ausfüllen des Registrierungsformulars darauf, einen registrierten Namen (DN) einzugeben, der mit dem des anfordernden CA übereinstimmt.
   b. Prüfen Sie den Status der Registrierungsanforderung.
   c. Befolgen Sie die Anweisung am Ende des Abschnitts, um die Vorabregistrierungsdatei zu speichern.
2. Übertragen Sie die Vorabregistrierungsdatei auf die Maschine, auf der sich der anfordernde CA der Hierarchie befindet.
3. Melden Sie sich bei Trust Authority als der Benutzer an, der das System auf der Maschine installiert hat, auf der sich der anfordernde CA befindet.
4. Führen Sie den Befehl CaCertRq aus, und zwar unter AIX über die Befehlszeile und unter Windows NT über die DOS-Eingabeaufforderung.

   Stellen Sie bei Ausführung des Befehls CaCertRq sicher, daß Sie den absoluten Pfad und den Namen der Vorabregistrierungsdatei eingeben. Informationen zur Befehlssyntax und Parameterbeschreibungen finden Sie im Abschnitt „Dienstprogramm CA Certification" auf Seite 103.

   Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (" ") setzen. Für den Befehl 'CaCertRq' beispielsweise würden Sie den Parameter -r *vorabregistrierungspfad* (mit eingebetteten Leerzeichen) folgendermaßen angeben:

   ```
   CaCertRq -d .companyA.com -h -r "c:\Program Files\IBM\Trust
        Auhority\ccprereg.reg" -P 1835 -W Secure99
   ```

IP-Adreßmaske angeben

Sie können ein gegenseitig zertifiziertes CA-Zertifikat anfordern, das die CA-Hierarchie eines anderen CA übernimmt und die Gültigkeit des Zertifikats auf die IP-Adressen einschränkt, die von Ihrem Unternehmen verwendet werden.

Im folgenden Beispiel ist das Betriebssystem AIX, Ihr Unternehmen verwendet IP-Adressen im Bereich von 9.0.0.0. bis 9.255.255.254, die Vorabregistrierungsdatei befindet sich im Pfad /tmp/ccprereg.reg, und das Kennwort lautet Secure99. Folgender Befehl plaziert den angegebenen Adressenbereich in der Liste zulässiger Unterverzeichnisstrukturen:

```
CaCertRq -i 9.0.0.0/255.0.0.0 -h -r  /tmp/ccprereg.reg -P 1835 -W Secure99
```

DNS-Adressen angeben

Sie können ein CA-Zertifikat anfordern, das die CA-Hierarchie eines anderen CA übernimmt und die Gültigkeit des Zertifikats auf eine Gruppe von DNS-Adressen einschränkt.

Im folgenden Beispiel wird das Betriebssystem Windows NT verwendet, alle Trust Authority-CA-Hosts verfügen über DNS-Adressen, die mit .companyA.com enden, Pfad und Dateiname der Vorabregistrierungsdatei lauten a:\ccprereg.reg, und das Kennwort lautet Secure99. Mit folgendem Befehl werden die angegebenen DNS-Adressen in der Liste der zulässigen Unterverzeichnisstrukturen plaziert:

```
CaCertRq -d .companyA.com -h -r a:\ccprereg.reg -P 1835 -W Secure99
```

Anmerkung: Beginnt eine DNS-Adresse mit einem Punkt, werden alle Hosts einbezogen, die mit dieser Unterzeichenfolge (einschließlich ".") enden. Diese Adressen werden in die Liste der Unterverzeichnisstrukturen aufgenommen. Beginnt die Adresse nicht mit einem Punkt, wird nur der Host einbezogen, dessen Name der Zeichenfolge entspricht.

Der Einschränkung ".companyA.com" entsprechen beispielsweise us.companyA.com, vnet.companyA.com und w3.software.companyA.com, jedoch nicht companyA.com (oder kidcompanyA.com) selbst. Der Einschränkung companyA.com entsprechen companyA.com, jedoch nicht us.companyA.com oder die übrigen Adressen. Daraus folgt, daß eine zulässige Unterverzeichnisstrukturen ohne führenden Punkt "." nur einen möglichen Knoten angibt. Angaben ohne einen führenden Punkt werden primär für nicht zulässige Unterverzeichnisstrukturen verwendet.

E-Mail-Adressen angeben

Sie können ein CA-Zertifikat anfordern, das die CA-Hierarchie eines anderen CA übernimmt und die Gültigkeit des Zertifikats auf eine Gruppe von E-Mail-Adressen einschränkt.

Im folgenden Beispiel wird das Betriebssystem AIX verwendet, alle Trust Authority-CA-Hosts verfügen über E-Mail-Adressen, die mit .us.companyA.com enden, Pfad und Dateiname der Vorabregistrierungsdatei lauten /tmp/ccprereg.reg, und das Kennwort lautet Secure99. Folgender Befehl plaziert die angegebenen E-Mail-Adressen in der Liste zulässiger Unterverzeichnisstrukturen:

```
CaCertRq -m .us.companyA.com -h -r /tmp/ccprereg.reg -P 1835 -W Secure99
```

Sie können ein CA-Zertifikat anfordern, das die CA-Hierarchie eines anderen CA übernimmt und die Gültigkeit des Zertifikats auf alle bis auf ein Element einer Gruppe von E-Mail-Adressen einschränkt. Im folgenden Beispiel hat der Trust Authority-CA-Host die E-Mail-Adresse outCA.us.companyA.com, Pfad und Dateiname der Vorabregistrierungsdatei lauten /tmp/ccprereg.reg, und das Kennwort lautet Secure99. Folgender Befehl plaziert die angegebene E-Mail-Adresse in der Liste nicht zulässiger Unterverzeichnisstrukturen:

```
CaCertRq -m .us.companyA.com -M outCA.us.companyA.com -h -r /tmp/ccprereg.reg -P 1835
   Secure99
```

URIs angeben

Sie können ein CA-Zertifikat anfordern, das die CA-Hierarchie eines anderen CA übernimmt und die Gültigkeit des Zertifikats auf eine Gruppe von URIs (Uniform Resource Identifiers, eine Kennungskategorie, die hauptsächlich aus URL-Adressen besteht) einschränkt. Im folgenden Beispiel wird das Betriebssystem Windows NT verwendet, alle Trust Authority-CA-Hosts verfügen über URIs, die mit .xyz.com enden, Pfad und Dateiname der Vorabregistrierungsdatei lauten a:\ccprereg.reg, und das Kennwort lautet Secure99. Folgender Befehl plaziert die angegebene URI in der Liste zulässiger Unterverzeichnisstrukturen:

```
CaCertRq -u .xyz.com -h -r a:\ccprereg.reg -P 1835 -W Secure99
```

Anmerkung: Der Knotenabschnitt der URI unterliegt den im Abschnitt „DNS-Adressen angeben" auf Seite 26 beschriebenen Regeln, sofern er keine IP-Adressen enthält. In diesem Fall wird er als exakte Übereinstimmung behandelt.

Verzeichniseinträge angeben

Sie können ein CA-Zertifikat anfordern, das die CA-Hierarchie eines anderen CA übernimmt und die Gültigkeit des Zertifikats auf eine Gruppe von Verzeichniseinträgen mit den gleichen RDNs (Relative Distinguished Names, relative registrierte Namen) einschränkt. Im folgenden Beispiel wird das Betriebssystem AIX verwendet, alle Trust Authority-CA-Hosts verfügen über RDNs, die den angegebenen RDNs (/C=US/O=companyA/OU=departmentB) entsprechen, Pfad und Dateiname der Vorabregistrierungsdatei lauten /tmp/ccprereg.reg, und das Kennwort lautet Secure99. Folgender Befehl plaziert den angegebenen RDN in der Liste der zulässigen Unterverzeichnisstrukturen:

```
CaCertRq -n "/C=US/O=companyA/OU=departmentB" -h -r /tmp/ccprereg.reg -P 1835
-W Secure99
```

Anmerkung: In Trust Authority wird für DNs folgendes Format verwendet:

/C=*Land*/O=*Unternehmen*/OU=*Unternehmenseinheit*/CN=*allgemeiner_Name*

Namenseinschränkungen ausschließen

Wenn Sie planen, als Teil Ihrer allgemeinen Hierarchielösung die hierarchischen CA-Zertifikate in Netscape Communicator herunterzuladen, sollten Sie die Markierung "-m .." mit dem Dienstprogramm CA Certification verwenden, um die Erweiterung für Namenseinschränkungen (Name Constraints) aus dem resultierenden CA-Zertifikat auszuschließen. Im folgenden Beispiel wird das Betriebssystem Windows NT ausgeführt, und es werden jeweils die Standardwerte für den Installationspfad, den Namen der Vorabregistrierungsdatei und das Systemkennwort von Trust Authority verwendet. Beispiel: Ein Exemplar eines solchen Befehls könnte folgendermaßen aussehen:

```
CaCertRq -m .. -h -r "c:\Program Files\IBM\Trust Authority\ccprereg.reg"
-P 1835 -W Secure99
```

CA-Server-Protokolle prüfen

Die Protokolle des CA-Servers zeichnen alle Transaktionen mit dem CA-Server auf. Sie können die Protokolle des CA-Servers an den nachfolgend beschriebenen Positionen prüfen.

Tabelle 6. Protokolle des CA-Servers

AIX-Standardpfad	Windows NT-Standardpfad	Beschreibung
/usr/lpp/iau/etc/TrustAuthority	c:\Program Files\IBM\Trust Authority\etc\TrustAuthority	Für Protokolldateinamen gilt der Stamm caSS.log. Für jede neue Protokolldatei wird die Erweiterung *xnnnnnn* inkrementell erhöht.

CA-Server-Status prüfen

Je nach Umgebung können Sie den Status des CA-Servers mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Root an.
  2. Prüfen Sie die Prozeßtabellen und suchen Sie nach folgender Zeichenfolge:

     ```
     irgAutoCa
     ```

     Finden Sie diesen Prozeß, fahren Sie mit Schritt 3 fort. Finden Sie diesen Prozeß nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 120 nach.
  3. Wechseln Sie in das Verzeichnis bin. Dieses Verzeichnis hat folgenden Standardpfad:

     ```
     /usr/lpp/iau/bin
     ```
  4. Prüfen Sie, ob Anschluß 1835 erfolgreich antwortet, indem Sie folgenden Befehl eingeben:

     ServerControl -i -c -k CA -n *Server* **-p 1835 -l "***Protokolldatei***"**

     Hierbei steht *Server*für den Namen des CA-Servers, der dem Anschluß 1835 zugeordnet ist, und *Protokolldatei* für den Namen der Datei, in der die Ergebnisse des Befehls ServerControl aufgezeichnet werden sollen.

     Ist die Antwort des geprüften Anschlusses erfolgreich, wird folgende Nachricht angezeigt:

     ```
     Es wurde
     festgestellt, daß der [CA]-Service auf dem Server am Anschluß 1835 ausgeführt wird.
     ```

     Hierbei steht *Server* für den Server, der dem Anschluß 1835 zugeordnet ist.

- Unter Windows NT:
  1. Melden Sie sich bei Windows NT als Systemadministrator an.
  2. Starten Sie den Task-Manager durch Drücken der Tastenkombination **Strg**, **Alt** und **Entf**.
  3. Wählen Sie die Registerkarte **Prozesse** aus.
  4. Suchen Sie nach dem Prozeß irgAutoCA.exe.

     Finden Sie diesen Prozeß, fahren Sie mit Schritt 5 fort. Finden Sie diesen Prozeß nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 120 nach.
  5. Wechseln Sie an der MS DOS-Eingabeaufforderung in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:

     ```
     c:\Program Files\IBM\Trust Authority\bin
     ```
  6. Prüfen Sie, ob Anschluß 1835 erfolgreich antwortet, indem Sie folgenden Befehl eingeben:

     ServerControl -i -c -k CA -n *Server* **-p 1835 -l "***Protokolldatei***"**

     Hierbei steht *Server*für den Namen des CA-Servers, der dem Anschluß 1835 zugeordnet ist, und *Protokolldatei* für den Namen der Datei, in der die Ergebnisse des Befehls ServerControl aufgezeichnet werden sollen.

     Ist die Antwort des geprüften Anschlusses erfolgreich, wird folgende Nachricht angezeigt:

     ```
     Es wurde
     festgestellt, daß der [CA]-Service auf dem Server am Anschluß 1835 ausgeführt wird.
     ```

     Hierbei steht *Server* für den Server, der dem Anschluß 1835 zugeordnet ist.

Aktivierung der CRL-Verteilungspunkte

Um die CRL-Verteilungspunkte zu aktivieren, gehen Sie folgendermaßen vor:

1. Melden Sie sich bei Ihrem Betriebssystem als Administrator an.
2. Stoppen Sie das Trust Authority-System.
3. Starten Sie den Editor iniEditor, und laden Sie die Konfigurationsdatei jonahca.ini.
4. Wählen Sie den Abschnitt **General** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **CertperDP** aus.
5. Ändern Sie im angezeigten Editierfeld den Wert in eine positive ganze Zahl ungleich Null.
6. Wählen Sie im Abschnitt **General** den Parameter **CRLDistName** aus.
7. Ändern Sie im angezeigten Editierfeld den Wert in einen aussagekräftigen Namen. In dem Namen muß **'%d'** erhalten bleiben.
8. Speichern Sie die Datei, und verlassen Sie den Editor iniEditor.
9. Starten Sie das Trust Authority-System.

CA-Server verwalten

In diesem Abschnitt werden Prozeduren für Betrieb und Verwaltung des Trust Authority Registrierungsstellen-Servers (RA-Server) erläutert. Der RA-Server verwaltet die Kommunikation zwischen RA Desktop und CA-Server. Er befindet sich zusammen mit seinem DB2-Datenbankexemplar auf einer lokalen Maschine.

Zur Verwaltung des RA-Servers müssen Sie in der Regel die nachfolgend beschriebenen Tasks ausführen:

- Verwenden Sie das Dienstprogramm zum Hinzufügen von RA-Benutzern (add_rauser), um dem System Benutzer als Registratoren (RA-Administratoren) hinzuzufügen.
- Verwenden Sie das Dienstprogramm zum Aktivieren der RA-Datenbankverschlüsselung (iauEnableRADBSec), um die Verschlüsselung der RA-Datenbank zu aktivieren.
- Verwenden Sie den Editor IniEditor, um folgende Änderungen an der Konfigurationsdatei jonahra.ini vorzunehmen:
  - Ändern des Anschlusses, der vom RA-Server überwacht wird.
  - Ändern des RA-Sendeaufrufintervalls.
  - Ändern des RA-Wiederholungsintervalls.
  - Ändern der RA-Einstellungen für die Kommunikation mit dem Directory.
- Prüfen der Protokolle des RA-Servers.
- Prüfen des Status des RA-Servers.

Registratoren hinzufügen

Sie sind für das Hinzufügen neuer Registratoren zum System verantwortlich. Ein Benutzer mit dem Status eines Registrators kann die Funktionen nutzen und auf die eingeschränkten Ressourcen zugreifen, die in einem der RA-Profile in der Konfigurationsdatei einer Trust Authority-Registrierungsfunktion definiert wurden. Um einen neuen Registrator hinzufügen zu können, müssen Sie selbst ein RA-Administrator sein. Dieser Abschnitt erläutert die Prozeduren zum erstmaligen Anfordern des Identitätsnachweises als RA-Administrator und zum Hinzufügen eines weiteren RA-Administrators.

Eigenen Benutzereintrag als ersten Registrator hinzufügen

Gehen Sie wie folgt vor, um sich selbst dem Trust Authority-System als Registrator hinzuzufügen:

1. Fordern Sie ein Browser-Zertifikat an, sofern Sie noch keines besitzen. Fahren Sie fort, wenn Sie dieses Zertifikat erhalten haben. Nähere Informationen hierzu finden Sie im *Benutzerhandbuch*.
2. Tragen Sie eine der folgenden Identifikationscodes ein:
   - Die Anforderungs-ID, die während der Browser-Registrierung für Sie generiert wurde.

     Wenn Sie sich erst kürzlich für ein Browser-Zertifikat registriert haben, verfügen Sie möglicherweise noch über diese ID.
   - Die Identitätsnachweis-UUID (eindeutige Benutzer-ID), die aufgrund der erfolgreichen Browser-Registrierung generiert wurde.

     Gehen Sie folgendermaßen vor, um Ihre Identitätsnachweis-UUID zu erhalten:

a. Starten Sie eine interaktive DB2-Befehlszeilensitzung. Verwenden Sie je nach Betriebssystem folgende Prozeduren:
   - Unter AIX:
     1) Geben Sie an der Eingabeaufforderung den Befehl `su` ein, um zum Eintrag des Benutzers mit Administratorberechtigung zu wechseln, der Trust Authority installiert hat.
     2) Geben Sie das Kennwort dieses Trust Authority-Benutzers ein.
     3) Geben Sie den Befehl **db2** ein, um die DB2-Sitzung zu starten.
     4) Geben Sie an der DB2-Eingabeaufforderung folgenden Befehl ein, um die Verbindung zur Datenbank herzustellen:

        ```
        connect to pkrfdb
        ```

        In diesem Beispiel wird die Standard-Registrierungsdatenbank pkrfdb verwendet.
   - Unter Windows NT:
     1) Wählen Sie in der Windows-Funktionsleiste die Option **Start → Programme → DB2 für Windows NT → Befehlszeilenprozessor** aus.
     2) Geben Sie an der Eingabeaufforderung den Befehl **DB2** ein.
     3) Geben Sie den Befehl **connect to pkrfdb** ein.

        In diesem Beispiel wird die Standard-Registrierungsdatenbank pkrfdb verwendet.

b. Geben Sie an der DB2-Eingabeaufforderung einen SQL-Befehl nach folgendem Muster ein:

   ```
   select last_name, first_name, credential_uuid, created_on from requests
      where last_name = 'IhrNachname' and first_name =
   'IhrVorname' and
      profile_name like '%BrowserCert%'
   ```

   Ist diese Abfrage erfolgreich, gibt das System den angeforderten Nachnamen, Vornamen, die Identitätsnachweis-UUID und die Zeitmarke aller entsprechenden Einträge zurück. In diesem Beispiel handelt es sich bei den zurückgegebenen Informationen um Angaben aus dem Anforderungssatz Ihres genehmigten Browser-Zertifikats.

c. Geben Sie den Befehl **quit** ein, um die DB2-Sitzung zu beenden.

3. Befolgen Sie die Anweisungen im Abschnitt „Einen Registrator hinzufügen" ab Schritt 3 auf Seite 36, um das Hinzufügen des eigenen Benutzereintrags als ersten Registrator abzuschließen.

Einen Registrator hinzufügen

Je nach den von Ihrem Unternehmen festgelegten Regeln kann eine Anforderung zum Hinzufügen eines Registrators auf verschiedene Weise gestellt werden, beispielsweise in Form eines informellen Telefongesprächs oder über einen formellen Antragsprozeß. Um als Registrator berechtigt werden zu können, muß der betreffende Benutzer in den meisten Unternehmen zunächst ein SSL-Browser-Zertifikat erhalten. Benutzer können Browser-Zertifikate anfordern, indem Sie die browsergestützten Standardregistrierungsanweisungen im Trust Authority *Benutzerhandbuch* befolgen.

Trust Authority bietet zum Hinzufügen von Registratoren das Befehlszeilendienstprogramm 'add_rauser'. Die Syntax dieses Befehls wird im Abschnitt „Dienstprogramm Add RA User" auf Seite 105 erläutert.

Gehen Sie nach Erhalt einer Anforderung wie folgt vor, um dem System einen Registrator hinzuzufügen:

1. Prüfen Sie den Status der Anforderung des SSL-Browser-Zertifikats des zukünftigen Registrators.

   Greifen Sie hierzu auf RA Desktop zu, und befolgen Sie die im Handbuch *Registration Authority Desktop* dokumentierten Prozeduren, um eine Abfrage zu übergeben und die Ergebnisse anzuzeigen.
2. Wurde ein Zertifikat ausgestellt, notieren Sie die ihm zugeordnete Identitätsnachweis-UUID.

   Anmerkung: Sie können auch die Anforderungs-ID verwenden, die während einer erfolgreichen Browser-Registrierung für ein Zertifikat generiert wurde.

   Um die Identitätsnachweis-UUID zu erhalten, lokalisieren Sie den Datenbankeintrag für das genehmigte Zertifikat, und zeigen Sie die Attribute dieses Eintrags an. Sie benötigen das Attribut der Identitätsnachweis-UUID, das Sie als einen Parameter des Befehls add_rauser verwenden müssen.
3. Führen Sie je nach Umgebung einen der folgenden Schritte aus:
   - Unter AIX:
     a. Wechseln Sie in das Stammverzeichnis der Installation. Geben Sie dazu bei Verwendung des Standard-Stammverzeichnisses folgenden Befehl ein:

        ```
        cd /usr/lpp/iau/bin
        ```

     b. Geben Sie einen Befehl nach folgendem Muster ein:

        ```
        ./add_rauser /usr/lpp/iau/pkrf/etc/domain.cfg YourDomain aBcXyZ==
             RAUser
        ```

        Dabei gilt:
        - `/usr/lpp/iau/pkrf/etc/domain.cfg` ist der Pfad des Standardstammverzeichnisses der Trust Authority-Installation und der Domänenkonfigurationsdatei.
        - *YourDomain* ist die Standard-Registrierungsdomäne.
        - `aBcXyZ==` ist entweder ein Beispiel einer Anforderungs-ID oder einer Identitätsnachweis-UUID.
        - `RAUser` ist das wahlfreie Zugriffsprofil.
   - Unter Windows NT:
     a. Wechseln Sie in das Stammverzeichnis der Installation. Geben Sie dazu bei Verwendung des Standard-Stammverzeichnisses folgenden Befehl ein:

        ```
        cd "c:\Program Files\IBM\Trust Authority\bin"
        ```

     b. Geben Sie einen Befehl nach folgendem Muster ein:

        ```
        add_rauser "c:\Program Files\IBM\Trust Authority\pkrf\etc\domain.cfg"
             YourDomain aBcXyZ== RAUser
        ```

        Dabei gilt:
        - `c:\Program Files\IBM\Trust Authority\pkrf\etc\domain.cfg` ist der Pfad des Standardstammverzeichnisses der Trust Authority-Installation und der Domänenkonfigurationsdatei.

          Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (″ ″) setzen.
        - *YourDomain* ist die Standard-Registrierungsdomäne.

– aBcXyZ== ist entweder ein Beispiel einer Anforderungs-ID oder einer Identitätsnachweis-UUID.
– RAUser ist das wahlfreie Zugriffsprofil.

Nach der Ausführung des Befehls wird eine Erfolgs- oder Fehlernachricht angezeigt.

Verschlüsselung für die RA-Datenbank aktivieren

Standardmäßig werden Informationen in der Registrierungsfunktion-Datenbank nicht verschlüsselt. Nach der Konfiguration des Trust Authority-Systems können Sie die Datenbankverschlüsselung durch Ausführen des Programms 'iauEnableRADBSec' aktivieren. Wenn Sie 'iauEnableRADBSec' ausführen, untersucht das Programm die Datei 'raconfig.cfg', um festzustellen, ob die Datenbankverschlüsselung bereits eingeschaltet ist. Falls nicht, wird die Verschlüsselung vom Programm 'iauEnableRADBSec' aktiviert. Ist die Aktivierung bereits erfolgt, gibt das Programm eine Nachricht aus und wird beendet. Das Programm 'iauEnableRADBSec' aktualisiert die RADATABASE- und afservice.RADB-Einträge in der Datei 'raconfig.cfg' mit den generierten Chiffrierschlüsseln. Anschließend werden die Werte für diese Einträge verschlüsselt und Base 64-codiert.

Anmerkung: Im Unterverzeichnis 'etc' des virtuellen Root-Installationsverzeichnisses, das für Ihre Registrierungsdomäne konfiguriert wurde (der im Setup Wizard angegebene Wert für das Root-Installationsverzeichnis), wird eine Sicherungskopie der Datei 'raconfig.cfg' erstellt. Der Name der Sicherungskopie lautet 'raconfig.cfg.ERADSBKUP'.

Verwenden Sie je nach Betriebssystem eine der folgenden Prozeduren, um die Verschlüsselung für die RA-Datenbank zu aktivieren:

- Unter AIX:
  1. Melden Sie sich als 'root' an:
     ```
     su - root
     ```
  2. Wechseln Sie in das Unterverzeichnis 'bin' Ihres Installationsverzeichnisses. In diesem Beispiel wird der folgende Standardinstallationspfad von Trust Authority verwendet:
     ```
     cd /usr/lpp/iau/bin
     ```
  3. Führen Sie das Programm 'iauEnableRADBSec' folgendermaßen aus. In diesem Beispiel werden der standardmäßige Registrierungsdomänenname und der standardmäßige Installationspfad von Trust Authority verwendet:
     ```
     ./iauEnableRADBSec -d YourDomain -r /usr/lpp/iau
     ```
- Unter Windows NT:
  1. Melden Sie sich als Trust Authority-Konfigurationsbenutzer an (normalerweise 'cfguser').
  2. Wechseln Sie in das Unterverzeichnis 'bin' Ihres Installationsverzeichnisses. In diesem Beispiel wird der folgende Standardinstallationspfad von Trust Authority verwendet:
     ```
     cd "c:\Program Files\IBM\Trust Authority\bin"
     ```
  3. Führen Sie das Programm 'iauEnableRADBSec' folgendermaßen aus. In diesem Beispiel werden der standardmäßige Registrierungsdomänenname und der standardmäßige Installationspfad von Trust Authority verwendet:
     ```
     iauEnableRADBSec -d YourDomain -r "c:\Program Files\IBM\Trust Authority"
     ```

Vom RA-Server überwachten Anschluß ändern

Der vom RA-Server überwachte Anschluß ist der Anschluß, der vom RA auf PKIX-Nachrichten hin überwacht wird. Gehen Sie wie folgt vor, um den Wert für diesen Anschluß zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei jonahra.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **Transport** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **TCPPort** aus.
5. Ändern Sie im angezeigten Editierfeld die Anschlußnummer.
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie IniEditor erneut und laden Sie die Konfigurationsdatei jonahca.ini. (Diese Datei kann sich je nach Installation auf einer lokalen oder einer fernen Maschine befinden).
8. Wählen Sie den Abschnitt **URLs** aus.
9. Ändern Sie im angezeigten Editierfeld die Anschlußnummer.
10. Speichern Sie die Datei und beenden Sie das Programm.
11. Starten Sie das Trust Authority-System.

RA-Sendeaufrufintervall ändern

Das RA-Sendeaufrufintervall ist die Zeit in Sekunden (s), Minuten (m) oder Stunden (h) zwischen den Abfragen der Arbeitsablaufswarteschlange durch den RA-Server. Die Elemente in dieser Warteschlange, deren Zuteilungszeit abgelaufen ist, werden für die Verarbeitung zugeteilt. Gehen Sie wie folgt vor, um das Sendeaufrufintervall zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei jonahra.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **Transport** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **PollInterval** aus.
5. Ändern Sie im angezeigten Editierfeld den Wert für das Sendeaufrufintervall.
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie das Trust Authority-System.

RA-Wiederholungsintervall ändern

Die Zeit zwischen den CA-Abfragen durch die RA in Sekunden (s), Minuten (m) oder Stunden (h), sofern der vom CA an die RA übermittelte Zeitpunkt für den Sendeaufruf vor der aktuellen Uhrzeit der RA liegt. Gehen Sie wie folgt vor, um das RA-Wiederholungsintervall zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei jonahra.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **Transport** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **RetryInterval** aus.
5. Ändern Sie im angezeigten Editierfeld den Wert für das Wiederholungsintervall.
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie das Trust Authority-System.

RA-Server-Protokolle prüfen

Sie können die Protokolle des RA-Servers an den im Abschnitt Tabelle 7 beschriebenen Positionen prüfen.

Tabelle 7. RA-Server-Protokolle

AIX-Standardpfad	Windows NT-Standardpfad	Beschreibung
/usr/lpp/iau/pkrf/Domains/YourDomain/logs/	c:\Program Files\IBM\Trust Authority\pkrf\Domains\YourDomain\logs\	Protokolldateien haben den Namen `irgrasvr` und die Erweiterung `.log.zufällige_Nummer`.

Anmerkung: In der gelieferten Form protokolliert der RA-Server nicht die Betriebsaktivität. Der Abschnitt „Fehlerbehebung mit aktivierter Nachrichtenerstellung auf Debug-Stufe" auf Seite 121 enthält Anweisungen und Informationen zu empfohlenen Stufen, wenn Sie die RA-Server-Protokollierung auf Debug-Stufe aktivieren wollen.

RA-Server-Status prüfen

Je nach Umgebung können Sie den Status des RA-Servers mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Root an.
  2. Prüfen Sie die Prozeßtabelle, und suchen Sie nach folgender Zeichenfolge:

     ```
     irgrasvr
     ```

     Finden Sie diesen Prozeß, fahren Sie mit Schritt 3 auf Seite 40 fort. Finden Sie diesen Prozeß nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung" auf Seite 120 nach.

3. Wechseln Sie in das Verzeichnis bin. Dieses Verzeichnis hat folgenden Standardpfad:

   ```
   /usr/lpp/iau/bin
   ```

4. Stellen Sie sicher, daß Anschluß 29783 erfolgreich antwortet und geben Sie hierzu folgenden Befehl ein:

   ServerControl -i -c -k RA -n *Server* **-p 29783 -l "***Protokolldatei***"**

   Hierbei steht *Server*für den Namen des RA-Servers, der dem Anschluß 29783 zugeordnet ist, und *Protokolldatei* für den Namen der Datei, in der die Ergebnisse des Befehls ServerControl aufgezeichnet werden sollen.

   Ist die Antwort des geprüften Anschlusses erfolgreich, wird folgende Nachricht angezeigt:

   ```
   Es wurde
   festgestellt, daß der [RA]-Service auf dem Server am Anschluß 29783 ausgeführt wird.
   ```

   Hierbei steht *Server* für den Server, der dem Anschluß 29783 zugeordnet ist.

- Unter Windows NT:
  1. Melden Sie sich bei Windows NT als Systemadministrator an.
  2. Starten Sie den Task-Manager durch Drücken der Tastenkombination **Strg**, **Alt** und **Entf**.
  3. Wählen Sie die Registerkarte **Prozesse** aus.
  4. Suchen Sie nach dem Prozeß irgrasvr.exe.

     Finden Sie diesen Prozeß, fahren Sie mit Schritt 5 fort. Finden Sie diesen Prozeß nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 120 nach.
  5. Wechseln Sie an der MS DOS-Eingabeaufforderung in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:

     ```
     c:\Program Files\IBM\Trust Authority\bin
     ```

  6. Stellen Sie sicher, daß Anschluß 29783 erfolgreich antwortet und geben Sie hierzu folgenden Befehl ein:

     ServerControl -i -c -k CA -n *Server* **-p 29783 -l "***Protokolldatei***"**

     Hierbei steht *Server*für den Namen des RA-Servers, der dem Anschluß 29783 zugeordnet ist, und *Protokolldatei* für den Namen der Datei, in der die Ergebnisse des Befehls ServerControl aufgezeichnet werden sollen.

     Ist die Antwort des geprüften Anschlusses erfolgreich, wird folgende Nachricht angezeigt:

     ```
     Es wurde
     festgestellt, daß der [RA]-Service auf dem Server am Anschluß 29783 ausgeführt wird.
     ```

     Hierbei steht *Server* für den Server, der dem Anschluß 29783 zugeordnet ist.

RA-Einstellungen für die Kommunikation mit dem Directory ändern

Der RA-Server kommuniziert mit dem IBM SecureWay Directory-Server, um den Registrierungsprozeß zu verwalten. In der Konfigurationsdatei des RA-Servers können folgende Werte geändert werden, um die Kommunikation zwischen RA und Directory zu beeinflussen:

- Host-Name und Anschluß des Directory-Servers
- Sendeintervall

RA-Einstellungen für Host-Namen und Anschluß des Directory-Servers ändern

Für eine effiziente Kommunikation mit dem Directory benötigt die RA den korrekten Host-Namen und den korrekten Anschluß, der vom Directory überwacht wird. Gehen Sie wie folgt vor, um den Host-Namen und den Anschluß, der von der RA für die Kommunikation mit dem Directory benötigt wird, zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei jonahra.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **LDAP** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **Server1** aus.
5. Ändern Sie im angezeigten Editierfeld die Werte für Host-Name und Anschlußnummer.
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie das Trust Authority-System.

RA-Einstellungen für das Sendeintervall des Directory-Servers ändern

Das Sendeintervall bezeichnet die Zeit, in der die RA nicht prüft, ob Informationen zum Senden an das Directory vorliegen. Zu diesen Informationen zählen beispielsweise neue Benutzerzertifikate oder neue CRLs.

Gehen Sie wie folgt vor, um das Sendeintervall der RA zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei jonahra.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **LDAP** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **PostInterval** aus.
5. Ändern Sie im angezeigten Editierfeld den Wert des Parameters PostInterval.
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie das Trust Authority-System.

Prüfsubsystem verwalten

Zur Verwaltung des Prüfsubsystems müssen Sie die Funktion eines Prüfadministrators übernehmen. Für einige dieser Verwaltungs-Tasks ist ein Kennwort erforderlich. Informationen zum Ändern des Kennworts für den Prüfadministrator finden Sie im Abschnitt „Trust Authority-Kennwörter ändern" auf Seite 5.

Der Prüf-Server ist ein Trust Authority-Prozeß, der Prüfereignisse von Trust Authority-Komponenten empfängt und diese in einem Prüfprotokoll aufzeichnet. Er befindet sich zusammen mit seinem DB2-Datenbankexemplar auf einer lokalen oder fernen Maschine. Der Prüf-Server muß sich auf der gleichen Maschine befinden, wie der CA-Server.

Zur Verwaltung des Prüfsubsystems müssen Sie in der Regel die nachfolgend beschriebenen Tasks ausführen:

- Verwenden der beiden Trust Authority-Datenbanksichten zum Anzeigen von Protokolleinträgen in der Prüfdatenbank.
- Verwenden der DB2 UDB-Tools zur Suche nach Protokolleinträgen oder zum Generieren von Prüfberichten.
- Verwenden des Editors IniEditor, um folgende Änderungen an der Konfigurationsdatei AuditClient.ini vorzunehmen:
  - Ändern des Anschlusses für den Prüf-Server.
  - Ändern der Sendeart für Ereignisse vom Prüf-Client.
- Verwenden des Editors IniEditor, um folgende Änderungen an der Konfigurationsdatei AuditServer.ini vorzunehmen:
  - Ändern des Anschlusses, der vom Prüf-Server überwacht wird.
  - Ändern der Anzahl von Wiederholungen, mit denen der Prüf-Client versucht, eine Verbindung mit dem Prüf-Server herzustellen.
  - Ändern der Zeit zwischen Verbindungsversuchen.
  - Ändern der Protokolleinstellungen für Ereignis-, Prüf-, Trace- und Fehlerprotokolle.
- Verwenden des Dienstprogramms 'Audit Archive and Sign' zur Archivierung und Unterzeichnung von Prüfprotokolldateien.
- Verwenden des Dienstprogramms 'Audit Integrity Check' zur Prüfung der Datenbankintegrität des Prüf-Servers und zur Archivierung von Dateien.
- Prüfen des Status des Prüf-Servers.
- Prüfen der Protokolle des Prüf-Servers.

Protokolleinträge anzeigen

Sie können sich die Protokolleinträge in der DB2-Prüfdatenbank mit Hilfe von zwei Trust Authority-Sichten anzeigen lassen. Diese Datenbanksichten zeigen alle derzeit in der Datenbank gespeicherten Protokolleinträge an. Die Protokolleinträge werden in der Datenbanktabelle audit_log gespeichert. Bei den meisten Spalten dieser Tabelle handelt es sich um kurze Integer-Codes, die auf andere Tabellen verweisen. Diese anderen Tabellen enthalten die vollständige Beschreibung oder die Namen der Felder des Protokolleintrags. (Diese Felder entsprechen in der Datenbank den Spalten einer Tabelle.) Informationen zu Feldnamen und Beschreibungen aller Tabellen im Prüfdatenbankschema finden Sie im Abschnitt „Daten der Prüfdatenbank" auf Seite 113.

Folgende Sichten sind verfügbar:

- viewar

  Dies ist die grundlegende Sicht, die den Zugriff auf alle Textbeschreibungen (ungekürzt) ermöglicht.

- viewar_t

  Diese Sicht entspricht der Sicht viewar, die Textspalten werden jedoch nach 40 Zeichen abgeschnitten.

  Anmerkung: Wenn Sie die Datenbank 'viewar_t' unter Windows NT über die Schnittstelle der DB2-Steuerzentrale abfragen, wird aufgrund des Abschneidens beim Auswählen der Option für den Beispielinhalt eine leere Ausgabe angezeigt. Die in diesem Abschnitt dokumentierte Prozedur bietet eine Möglichkeit, dieses Problem zu umgehen.

Die Sichten verfügen über die im Abschnitt Tabelle 8 auf Seite 44 erläuterten Spaltennamen.

Tabelle 8. Spaltenbeschreibungen der Sichten für die Trust Authority-Prüfdatenbank

Spaltenname	Beschreibung	Datentyp
serial_num	Die Seriennummer des Protokolleintrags	integer
sourcetime	Die Zeitmarke, die angibt, wann das Prüfereignis durch den Client erstellt wurde.	timestamp
createtime	Die Zeitmarke, die angibt, wann der Protokolleintrag erstellt wurde.	timestamp
Ereignis	Der Name des Ereignisses	varchar
source	Der Prüf-Client, der das Prüfereignis generiert hat.	varchar
component	Die Komponentenart des Prüf-Clients, der das Prüfereignis generiert hat.	varchar
auth_entity	Die Entität, die das Prüfereignis berechtigt hat.	varchar
auth_role	Der Aufgabenbereich der Entität, die das Prüfereignis berechtigt hat.	varchar
affected_entity	Die Kennung der Entität, die von einem Prüfereignis betroffen ist.	varchar
affected_entity_type	Die Art der betroffenen Entität.	varchar
storage_media	Das dem Prüfereignis zugeordnete Speichermedium.	varchar
extra_info	Dem Prüfereignis zugeordnete Zusatzinformationen.	varchar

Gehen Sie wie folgt vor, um sich die Sätze in der Trust Authority-Prüfdatenbank anzeigen zu lassen:

1. Melden Sie sich bei Trust Authority als der Benutzer an, der Trust Authority installiert hat.
2. Starten Sie eine interaktive DB2-Befehlszeilensitzung.

   Anmerkung: Wenn Sie Windows NT ausführen, hat eine während des Installationsabschlusses definierte Variable der Zeichenumsetztabelle möglicherweise dazu geführt, daß in den char- und varchar-Spalten im DB2-Befehlsfenster unleserliche Zeichen angezeigt werden. Um dies zu beheben, geben Sie vor der Eingabe von DB2 SQL-Anweisungen die folgenden Befehle ein:

   ```
   set DB2CODEPAGE=
   db2 terminate
   ```

   Starten Sie die DB2-Sitzung anschließend erneut.
3. Geben Sie an der DB2-Befehlszeile den folgenden Befehl ein, um eine Verbindung zur Prüfdatenbank herzustellen:

   ```
   connect to
   Name_Ihrer_Prüfdatenbank
   ```

   Geben Sie beispielsweise für die Datenbank namens adtdb folgenden Befehl ein:

   ```
   connect to adtdb
   ```
4. Fragen Sie die Datenbank wie nachfolgend beschrieben mit Hilfe einer Trust Authority-Sicht ab.
   - Geben Sie für eine Abfrage mit der Sicht viewvar folgenden Befehl ein:

     ```
     "select * from viewvar"
     ```
   - Geben Sie für eine Abfrage mit der Sicht viewvar_t folgenden Befehl ein:

     ```
     "select * from viewvar_t"
     ```

     Das System zeigt für alle Einträge der Prüfdatenbank die im Abschnitt Tabelle 8 auf Seite 44 beschriebenen Spalten an.
5. Verwenden Sie zum Filtern der Sicht für die Protokolleinträge die SQL-Klausel `where`. Geben Sie beispielsweise folgenden Befehl ein, um Einträge auf einen bestimmten Datumsbereich zu beschränken:

   ```
   "select * from viewar where sourcetime between '1999-07-01-08.00.00' and
    '1999-07-02-08.00.00'"
   ```

   Nähere Informationen zur SQL-Anweisung `select` finden Sie im Handbuch *IBM DB2 Universal Database SQL Reference, Version 5.2*. Nähere Informationen zum Befehl db2 finden Sie im Handbuch *IBM DB2 Universal Database Command Reference, Version 5.2*.

Protokolleinträge suchen

Anweisungen zum Suchen nach Protokolleinträgen finden Sie im Handbuch *IBM DB2 Universal Database SQL Reference, Version 5.2*.

Prüf-Server-Anschluß im Prüf-Client ändern

Der Prüf-Server-Anschluß ist der Anschluß, der vom Prüf-Server auf neue Verbindungen vom Prüf-Client hin überwacht wird. Für eine effiziente Kommunikation zwischen Prüf-Client und Prüf-Server muß der Prüf-Client über den korrekten Anschluß des Prüf-Servers verfügen. Gehen Sie wie folgt vor, um die Werte für den Anschluß des Prüf-Servers in der Konfigurationsdatei des Prüf-Clients zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei AuditClient.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **Connection** (Verbindung) aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **Port** (Anschluß) aus.
5. Ändern Sie im angezeigten Editierfeld die Anschlußnummer des Prüf-Servers.
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie das Trust Authority-System.
8. Stellen Sie sicher, daß der geänderte Anschlußwert dem Wert des Parameters acceptor.arg in der Datei AuditServer.ini entspricht. Diese Datei befindet sich auf dem Prüf-Server.

Sendeweise für Ereignisse vom Prüf-Client ändern

Der Prüf-Client sendet Prüfereignisse an den Prüf-Server. Sie können das Senden bestimmter Ereignisse an den Prüf-Server unterbinden, indem Sie in der Datei AuditClient.ini eine Prüfmaske definieren. Einige Ereignisse müssen jedoch immer gesendet werden. Informationen zu verbindlichen und wahlfreien Prüfereignissen finden Sie im Abschnitt „Prüfereignisse" auf Seite 110. Darüber hinaus können Sie auch die Anzahl der Wiederholungsversuche nach dem ersten Sendeversuch des Prüf-Clients an den Prüf-Server definieren. Sie können auch die Zeit in Millisekunden angeben, die zwischen den Wiederholungsversuchen für das Herstellen einer Verbindung zum Server gewartet werden soll.

Prüfmaske definieren

Gehen Sie wie folgt vor, um eine Prüfmaske zu definieren:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei AuditClient.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **CA**, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **ExcludedEvents** aus.
5. Fügen Sie im angezeigten Editierfeld die Namen der vom CA generierten Prüfereignisse hinzu, die vom Prüf-Client zurückgehalten werden sollen. Die Namen der Prüfereignisse müssen durch Kommas getrennt werden. Geben Sie nur wahlfreie Ereignisse an.
6. Wählen Sie den Abschnitt **RA** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **ExcludedEvents** aus.
7. Fügen Sie im angezeigten Editierfeld die Namen der von der RA generierten Prüfereignisse hinzu, die vom Prüf-Client zurückgehalten werden sollen. Die Namen der Prüfereignisse müssen durch Kommas getrennt werden. Geben Sie nur wahlfreie Ereignisse an. Informationen zu den Namen von Prüfereignissen finden Sie im Abschnitt „Prüfereignisse" auf Seite 110.
8. Speichern Sie die Datei und beenden Sie das Programm.
9. Starten Sie das Trust Authority-System.

Anzahl der Wiederholungen für das Senden von Ereignissen ändern

Gehen Sie wie folgt vor, um die Anzahl von Wiederholungsversuchen nach dem ersten Sendeversuch des Prüf-Clients zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei AuditClient.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **Connection** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **Retries** aus.
5. Ändern Sie im angezeigten Editierfeld den Wert des Parameters Retries.

6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie das Trust Authority-System.

Intervall zwischen Wiederholungsversuchen ändern

Um das Intervall zwischen Wiederholungsversuchen zu ändern, gehen Sie wie folgt vor:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei AuditClient.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **Connection** (Verbindung) aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **Timer** aus.
5. Ändern Sie im angezeigten Editierfeld den Wert des Parameters 'Timer'.
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie das Trust Authority-System.

Vom Prüf-Server überwachten Anschluß ändern

Der Prüf-Server-Anschluß ist der Anschluß, der vom Prüf-Server auf neue Verbindungen vom Prüf-Client hin überwacht wird. Gehen Sie wie folgt vor, um die Werte für den Anschluß des Prüf-Servers in der Konfigurationsdatei des Prüf-Servers zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei AuditServer.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **Server Port**, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **acceptor.arg** aus.
5. Ändern Sie im angezeigten Editierfeld die Anschlußnummer.
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie das Trust Authority-System.
8. Stellen Sie sicher, daß der geänderte Server-Anschluß an alle lokalen und fernen Dateien vom Typ AuditClient.ini weitergegeben wird. Nähere Informationen hierzu finden Sie im Abschnitt „Prüf-Server-Anschluß im Prüf-Client ändern" auf Seite 46.

Anzahl der Bindungsversuche zwischen Prüf-Server und Prüf-Client ändern

Gehen Sie wie folgt vor, um die Anzahl der Bindungsversuche des Prüf-Clients zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei AuditServer.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **Server Port** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **acceptor.init.retries** aus.
5. Ändern Sie im angezeigten Editierfeld die Anzahl der Bindungsversuche. Der Standardwert lautet 3.
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie das Trust Authority-System.

Intervall zwischen Bindungsversuchen ändern

Gehen Sie wie folgt vor, um das Intervall zwischen den Bindungsversuchen des Prüf-Clients zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei AuditServer.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **Server Port** aus, zeigen Sie die zugehörigen Unterabschnitte an, und wählen Sie anschließend den Parameter **acceptor.init.delay** aus.
5. Ändern Sie im angezeigten Editierfeld die Zeit (in Sekunden) zwischen den Bindungsversuchen. Der Standardwert lautet 3. (Das Programm geht von Sekunden aus.)
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie das Trust Authority-System.

Protokolleinstellungen ändern

Sie können die Einstellungen in der Datei AuditServer.ini für folgende Protokolltypen ändern:

- Ereignisprotokoll - Zur Aufzeichnung von Prüfereignissen
- Prüfprotokoll - Zur Speicherung integritätsgeschützter Prüfereignisse in der Datenbank
- Trace-Protokoll - Zur Aufzeichnung von Programmaktivitäten
- Fehlerprotokoll - Für Fehlernachrichten

Aufzeichnungsart für Prüfereignisse ändern

Das Ereignisprotokoll ist eine Datei zur Aufzeichnung von Ereignissen. Sie können folgende Konfigurationsparameter ändern:

- Den Dateinamen und den Pfad des Ereignisprotokolls
- Die Markierung, die angibt, ob Daten an das bereits vorhandene Ereignisprotokoll angefügt werden oder ob diese überschrieben wird.

Gehen Sie wie folgt vor, um die Einstellungen für das Aufzeichnen von Ereignissen zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei AuditServer.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen und Sie den Abschnitt **Event Log** aus, und zeigen Sie die zugehörigen Unterabschnitte an. Weitere Schritte:
   - Gehen Sie wie folgt vor, um den Pfad oder den Dateinamen des Ereignisprotokolls zu ändern:
     a. Wählen Sie den Parameter **event.log.filename** aus.
     b. Ändern Sie im angezeigten Editierfeld den Pfad oder den Dateinamen.
   - Gehen Sie wie folgt vor, um die Markierung zu ändern, die angibt, ob das Daten an das bereits vorhandende Ereignisprotokoll angefügt werden oder ob dieses überschrieben wird:
     a. Wählen Sie den Parameter **event.log.append** aus.
     b. Ändern Sie im angezeigten Editierfeld den Wert des Parameters. Der Wert lautet **true** zum Anfügen oder **false** zum Überschreiben.
5. Speichern Sie die Datei und beenden Sie das Programm.
6. Starten Sie das Trust Authority-System.

Protokollierung von Prüfereignissen in der Datenbank ändern

Das Prüfprotokoll besteht aus einer Reihe von integritätsgeschützten Datenbanktabellen, die zur Speicherung von Prüfereignissen verwendet werden. Das Prüfprotokoll enthält pro Prüfereignis einen Protokolleintrag. Sie können folgende Konfigurationsparameter ändern:

- Die Anzahl der zulässigen Versuche zur Herstellung einer Verbindung mit der Prüfprotokolldatenbank
- Die Anzahl der zulässigen Versuche zur Aktualisierung der Prüfprotokolldatenbank
- Den zulässigen Zeitlimitüberschreitungswert (in Sekunden) zur Aktualisierung des Prüfprotokolls

Gehen Sie wie folgt vor, um die Einstellungen für das Protokollieren von Prüfereignissen zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei AuditServer.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie

bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.

4. Wählen Sie den Abschnitt **Audit** aus, und zeigen Sie die zugehörigen Unterabschnitte an. Weitere Schritte:
   - Gehen Sie wie folgt vor, um die Anzahl der zulässigen Versuche zur Herstellung einer Verbindung mit der Prüfprotokolldatenbank zu ändern:
     a. Wählen Sie den Parameter **audit.log.connect.retries** aus.
     b. Ändern Sie im angezeigten Editierfeld den Wert des Parameters. Sie müssen einen Integer-Wert eingeben.
   - Gehen Sie wie folgt vor, um die Anzahl der zulässigen Versuche zur Aktualisierung des Prüfprotokolls zu ändern:
     a. Wählen Sie den Parameter **audit.log.update.retries** aus.
     b. Ändern Sie im angezeigten Editierfeld den Wert des Parameters. Sie müssen einen Integer-Wert eingeben.
   - Gehen Sie wie folgt vor, um den zulässigen Zeitlimitüberschreitungswert zur Aktualisierung des Prüfprotokolls zu ändern:
     a. Wählen Sie den Parameter **audit.log.timeout** aus.
     b. Ändern Sie im angezeigten Editierfeld den Wert des Parameters. Sie müssen ein Zeitintervall eingeben.
5. Speichern Sie die Datei und beenden Sie das Programm.
6. Starten Sie das Trust Authority-System.

Einstellungen für das Trace-Protokoll ändern

Das Trace-Protokoll enthält Aufzeichnungen zur Ausführung eines Computerprogramms. Es gibt die Reihenfolge der Ausführung von Anweisungen wider. Dieses Protokoll wird primär zur Fehlerbehebung verwendet. Sie können folgende Konfigurationsparameter ändern:

- Aktivieren/Inaktivieren der Trace-Funktion
- Die Trace-Stufe
- Dateiname und Pfad des Trace-Protokolls
- Die Markierung, die angibt, ob Daten an die bereits vorhandene Trace-Datei angefügt werden oder ob diese überschrieben wird.

Gehen Sie wie folgt vor, um die Einstellungen für das Trace-Protokoll zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei AuditServer.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **Trace** aus und zeigen Sie die zugehörigen Unterabschnitte an. Weitere Schritte:
   - Gehen Sie wie folgt vor, um die Trace-Funktion zu aktivieren oder zu inaktivieren:
     a. Wählen Sie den Parameter **trace.enable** aus.

b. Ändern Sie im angezeigten Editierfeld den Wert des Parameters. Sie müssen zum Aktivieren die Zeichenfolge **true** und zum Inaktivieren die Zeichenfolge **false** eingeben.

- Gehen Sie wie folgt vor, um die Trace-Stufe zu ändern:
  a. Wählen Sie den Parameter **trace.level.name** aus.
  b. Ändern Sie im angezeigten Editierfeld den Wert des Parameters. Sie müssen eine Zeichenfolge eingeben. Eine Liste der Trace-Stufen finden Sie im Abschnitt „Trace-Stufen" auf Seite 97.
- Gehen Sie wie folgt vor, um Dateiname und Pfad des Trace-Protokolls zu ändern:
  a. Wählen Sie den Parameter **trace.log.filename** aus.
  b. Ändern Sie im angezeigten Editierfeld den Wert des Parameters. Sie müssen eine Zeichenfolge eingeben.
- Gehen Sie wie folgt vor, um die Markierung zu ändern, die angibt, ob Daten an die bereits vorhandene Trace-Datei angefügt werden oder ob diese überschrieben wird.
  a. Wählen Sie den Parameter **trace.log.append** aus.
  b. Ändern Sie im angezeigten Editierfeld den Wert des Parameters. Der Wert lautet **true** zum Anfügen oder **false** zum Überschreiben.

5. Speichern Sie die Datei und beenden Sie das Programm.
6. Starten Sie das Trust Authority-System.

Namen und Pfad der Fehlerprotokolldatei ändern

Das Fehlerprotokoll enthält Fehlernachrichten des Prüfsubsystems. Gehen Sie wie folgt vor, um den Dateinamen und den Pfad des Fehlerprotokolls zu ändern:

1. Melden Sie sich bei Ihrem Betriebssystem als Systemadministrator an.
2. Stoppen Sie das Trust Authority-System. Lesen Sie gegebenenfalls die Anweisungen unter „Server-Komponenten starten und stoppen" auf Seite 7.
3. Starten Sie den Editor IniEditor und laden Sie die Konfigurationsdatei AuditClient.ini. Informationen zum Starten und Verwenden von IniEditor finden Sie bei Bedarf im Abschnitt „IniEditor zum Ändern von Konfigurationsdateien verwenden" auf Seite 9. Informationen zu den Dateipositionen unter AIX und Windows NT finden Sie im Abschnitt Tabelle 1 auf Seite 10.
4. Wählen Sie den Abschnitt **Error** aus, zeigen Sie die zugehörigen Unterabschnitte an und wählen Sie anschließend den Parameter **error.log.filename** aus.
5. Ändern Sie im angezeigten Editierfeld den Wert des Parameters.
6. Speichern Sie die Datei und beenden Sie das Programm.
7. Starten Sie das Trust Authority-System.

Prüfberichte generieren

Anweisungen zum Generieren von Prüfberichten finden Sie im Handbuch *IBM DB2 Universal Database SQL Reference, Version 5.2*.

Prüfprotokolldateien archivieren und unterzeichnen

Mit dem Trust Authority-Tool 'Audit Archive and Sign' können Sie Prüfprotokolldateien archivieren und unterzeichnen. Dieses Tool archiviert die Tabellen der Datenbank des Prüf-Servers, die Prüfsätze enthalten. Die Tabellen werden mit Hilfe des DB2-Exportdienstprogramms in einer Datei archiviert. Anschließend wird die Datei unterzeichnet. Alle Prüfsätze werden nach erfolgreicher Archivierung aus der Datenbank entfernt, wenn die Option -n nicht angegeben wird.

Anmerkung: Das Trust Authority-System muß vor der Ausführung dieses Dienstprogramms nicht heruntergefahren werden.

Angenommen, Sie verwenden den standardmäßigen Trust Authority-Installationspfad. Sie möchten die aktuellen Prüfsätze der Datenbank des Prüf-Servers in der Datei meine.datei archivieren und diese Datei unterzeichnen. Die Prüfsätze sollen jedoch nicht aus der Datenbank entfernt werden. Gehen Sie wie folgt vor:

1. Melden Sie sich bei Trust Authority als Konfigurationsbenutzer an der Maschine an, auf der die Trust Authority-CA- und Prüf-Server-Komponente installiert ist.

   Der empfohlene Benutzername, der gleichzeitig auch der Standardbenutzername ist, lautet **cfguser**. Wenn Trust Authority unter Windows NT installiert ist, wurde vom jeweiligen Unternehmen möglicherweise ein anderer Benutzername verwendet.
2. Geben Sie in der Befehlszeile Ihrer Umgebung folgenden Befehl ein:
   - Unter AIX:

     ```
     AuditArchiveAndSign -c /usr/lpp/iau/etc/TrustAuthority/AuditServer.ini -n
          /usr/lpp/iau/arc/meine.datei
     ```

   - Unter Windows NT:

     ```
     AuditArchiveAndSign -c "d:\Program Files\IBM\Trust Authority\etc\TrustAuthority\
        AuditServer.ini" -n "d:\Program Files\IBM\Trust
     Authority\arc\meine.datei"
     ```
3. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

   Die Ergebnisse werden auf der Standardausgabeeinheit angezeigt. Die Archivierungsdatei erhält die Erweiterung .ixf.

Informationen zur Befehlssyntax und Parameterbeschreibungen finden Sie im Abschnitt „Dienstprogramm Audit Archive and Sign” auf Seite 107.

Integrität der Datenbank des Prüf-Servers und der Archivierungsdateien prüfen

Trust Authority bietet ein Befehlszeilendienstprogramm, mit dem die Datenbank des Prüf-Servers und die archivierten Prüfdateien auf Manipulationen geprüft werden können. Dieses Tool trägt die Bezeichnung 'Audit Integrity Check'.

Anmerkung: Das Trust Authority-System muß vor der Ausführung dieses Dienstprogramms nicht heruntergefahren werden.

Mit diesem Dienstprogramm können Sie Manipulationen in den nachfolgenden Daten-Repositories lokalisieren. Sie werden in jedem Fall zur Eingabe des Kennworts für den Prüfadministrator [KeyStore-PIN] aufgefordert.

- Datenbank des Prüf-Servers
- Eine oder mehrere Prüf-Server-Archivierungsdateien
- Alle Archivierungsdateien in einem bestimmten Verzeichnis

Angenommen, Sie verwenden AIX und den Trust Authority-Standardpfad für Konfigurationsdateien. Melden Sie sich bei Trust Authority als Konfigurationsbenutzer (cfguser) an der Maschine an, auf der die Trust Authority-CA- und Prüf-Server-Komponente installiert ist. Sie möchten die nachfolgenden Komponenten nach Manipulationen durchsuchen.

- Gehen Sie wie folgt vor, um die Datenbank des Prüf-Servers zu prüfen:

1. Geben Sie an der AIX-Befehlszeile folgenden Befehl ein:

   ```
   AuditIntegrityCheck -c /usr/lpp/iau/etc/TrustAuthority/
      AuditServer.ini -d
   ```

2. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

   Die Ergebnisse werden auf der Standardausgabeeinheit angezeigt.

- Gehen Sie wie folgt vor, um eine oder mehrere Archivierungsdateien des Prüf-Servers zu prüfen:

  1. Geben Sie an der AIX-Befehlszeile folgenden Befehl ein:

     ```
     AuditIntegrityCheck -c /usr/lpp/iau/etc/TrustAuthority/AuditServer.ini
         -a /usr/lpp/iau/arc/archive1_my.file
     ```

  2. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

     Dieser Befehl prüft Dateien mit dem Pfadpräfix /usr/lpp/iau/arc/archive1_my.file und den Erweiterungen .ixf und .sig. Die Erweiterung .ixf kennzeichnet Dateien im von DB2 generierten Exportformat. Die Erweiterung .sig kennzeichnet eine vom Prüfsubsystem generierte Unterschriftsdatei.

- Gehen Sie wie folgt vor, um alle Archivierungsdateien in einem bestimmten Verzeichnis zu prüfen (in diesem Fall /usr/lpp/iau/arc/):

  1. Geben Sie an der AIX-Befehlszeile folgenden Befehl ein:

     ```
     AuditIntegrityCheck -c /usr/lpp/iau/etc/TrustAuthority/AuditServer.ini
         -A /usr/lpp/iau/arc/
     ```

  2. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

     Dieser Befehl prüft im angegebenen Verzeichnis alle Dateien mit der Erweiterung .ixf.

Angenommen, Sie verwenden Windows NT und den Trust Authority-Standardpfad für Konfigurationsdateien. Melden Sie sich bei Trust Authority als Konfigurationsbenutzer an der Maschine an, auf der die Trust Authority-CA- und Prüf-Server-Komponente installiert ist. Sie möchten die nachfolgenden Komponenten nach Manipulationen durchsuchen.

- Gehen Sie wie folgt vor, um die Datenbank des Prüf-Servers zu prüfen:

  1. Geben Sie an der DOS-Eingabeaufforderung (in diesem Fall c:) folgenden Befehl ein:

     ```
     AuditIntegrityCheck -c "c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\
        AuditServer.ini" -d
     ```

  2. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

     Die Ergebnisse werden auf der Standardausgabeeinheit angezeigt.

- Gehen Sie wie folgt vor, um eine oder mehrere Archivierungsdateien des Prüf-Servers zu prüfen:

  1. Geben Sie an der DOS-Eingabeaufforderung (in diesem Fall c:) folgenden Befehl ein:

     ```
     AuditIntegrityCheck -c "c:\Program Files\IBM\Trust Authority\
        etc\TrustAuthority\AuditServer.ini" -a "c:\Program Files\IBM\Trust Authority\
        arc\archive1_meine.datei"
     ```

  2. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

     Dieser Befehl prüft alle Dateien mit dem Pfadpräfix \Program Files\IBM\Trust Authority\arc\archive1_my.file und den Erweiterungen .ixf

und .sig. Die Erweiterung .ixf kennzeichnet Dateien im von DB2 generierten Exportformat. Die Erweiterung .sig kennzeichnet eine vom Prüfsubsystem generierte Unterschriftsdatei. Die exportierten Dateien werden also unterzeichnet, und die Unterschrift wird in der Datei mit der Erweiterung .sig gespeichert.

- Gehen Sie wie folgt vor, um alle Archivierungsdateien in einem bestimmten Verzeichnis zu prüfen (in diesem Fall c:\Program Files\IBM\Trust Authority\arc\):
  1. Geben Sie an der DOS-Eingabeaufforderung (in diesem Fall c:) folgenden Befehl ein:

     ```
     AuditIntegrityCheck -c c:\Program Files\IBM\Trust Authority\etc\
          TrustAuthority\AuditServer.ini -A c:\Program Files\IBM\Trust Authority\arc\
     ```

  2. Wenn das System Sie zur Eingabe eines Kennworts (KeyStore-PIN) auffordert, geben Sie das Kennwort des Prüfadministrators ein.

     Dieser Befehl prüft im angegebenen Verzeichnis alle Dateien einschließlich der Dateien mit den Erweiterungen .ixf und .sig.

Informationen zur Befehlssyntax und Parameterbeschreibungen finden Sie im Abschnitt „Dienstprogramm Audit Integrity Check" auf Seite 107.

Status des Prüf-Servers prüfen

Je nach Umgebung können Sie den Status des Prüf-Servers mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Root an.
  2. Prüfen Sie die Prozeßtabelle, und suchen Sie nach folgender Zeichenfolge:

     ```
     java
     ```

     Finden Sie diesen Prozeß, fahren Sie mit Schritt 3 fort. Finden Sie diesen Prozeß nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung" auf Seite 120 nach.
  3. Wechseln Sie in das Verzeichnis bin. Dieses Verzeichnis hat folgenden Standardpfad:

     ```
     /usr/lpp/iau/bin
     ```

  4. Prüfen Sie, ob der Anschluß (in diesem Fall Anschluß 59998) erfolgreich antwortet, indem Sie folgenden Befehl eingeben:

     ServerControl -i -c -k AUDIT -n
     Server **-p 59998 -l**
     "*Protokolldatei***"**

     Hierbei steht *Server*für den Namen des Prüf-Servers, der mit dem angegebenen Anschluß (in diesem Fall Anschluß 59998) zugeordnet ist, und *Protokolldatei* für den Namen der Datei, in der die Ergebnisse des Befehls ServerControl aufgezeichnet werden sollen.

     Ist die Antwort des geprüften Anschlusses erfolgreich, wird folgende Nachricht angezeigt:

     ```
     Der Prüf-Server wird momentan ausgeführt.
     ```

     Hierbei steht *Server* für den Server, der dem Anschluß 59998 zugeordnet ist.
- Unter Windows NT:
  1. Melden Sie sich bei Windows NT als Systemadministrator an.

2. Starten Sie den Task-Manager durch Drücken der Tastenkombination **Strg**, **Alt** und **Entf**.
3. Wählen Sie die Registerkarte **Prozesse** aus.
4. Suchen Sie nach dem Prozeß java.exe.

   Finden Sie diesen Prozeß, fahren Sie mit Schritt 5 fort. Finden Sie diesen Prozeß nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 120 nach.
5. Wechseln Sie an der MS DOS-Eingabeaufforderung in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:

   ```
   c:\Program Files\IBM\Trust Authority\bin
   ```
6. Prüfen Sie, ob der Anschluß (in diesem Fall Anschluß 59998) erfolgreich antwortet, indem Sie folgenden Befehl eingeben:

   ServerControl -i -c -k AUDIT -n
   Server **-p 59998 -l**
   "*Protokolldatei***"**

   Hierbei steht *Server*für den Namen des Prüf-Servers, der dem Anschluß 59998 zugeordnet ist, und *Protokolldatei* für den Namen der Datei, in der die Ergebnisse des Befehls ServerControl aufgezeichnet werden sollen.

   Ist die Antwort des geprüften Anschlusses erfolgreich, wird folgende Nachricht angezeigt:

   ```
   Der Prüf-Server wird momentan ausgeführt.
   ```

   Hierbei steht *Server* für den Server, der dem Trust Authority-Standardanschluß 59998 zugeordnet ist.

Prüf-Server-Protokolle prüfen

Die Protokolle des Prüf-Servers zeichnen alle Transaktionen mit dem Prüf-Server auf. Sie können die Protokolle des Prüf-Servers an den nachfolgend beschriebenen Positionen prüfen.

Tabelle 9. Protokolle des Prüf-Servers

AIX-Standardpfad	Windows NT-Standardpfad	Beschreibung
/usr/lpp/iau/logs/smevents.log	c:\Program Files\IBM\Trust Authority\logs\smevents.log	Das Ereignisprotokoll des Prüf-Servers zur Aufzeichnung von Prüfereignissen.
/usr/lpp/iau/logs/iausmd.log	c:\Program Files\IBM\Trust Authority\logs\iausmd.log	Das Trace-Protokoll des Prüf-Servers zur Aufzeichnung von Programmaktivitäten.
/usr/lpp/iau/logs/iausmd.err	c:\Program Files\IBM\Trust Authority\logs\iausmd.err	Das Fehlerprotokoll des Prüf-Servers zur Aufzeichnung von Fehlernachrichten.

DB2-Datenbanken verwalten

In diesem Abschnitt werden grundlegende Prozeduren für Betrieb und Verwaltung von DB2-Datenbanken erläutert. Nähere Informationen hierzu finden Sie in der DB2 UDB-Dokumentation.

Trust Authority verwendet die im Abschnitt Tabelle 10 aufgeführten Tabellen.

Tabelle 10. Datenbankpositionen

Exemplar	Datenbankname	Beschreibung
cfgusr	cfgdb	Die Trust Authority-Standard-Konfigurationsdatenbank
cfgusr	ibmdb	Die CA-Standarddatenbank
cfgusr	pkrfdb	Die Standard-Registrierungsdatenbank
cfgusr	adtdb	Die Standard-Prüfdatenbank
ldapInst	ldapdb	Die Standard-Directory-Datenbank bei Installation mit Trust Authority. Wenn Sie ein vorhandenes Verzeichnis verwenden, wird diese Position von Ihrem Unternehmen festgelegt.

Status von DB2-Datenbanken prüfen

Je nach Umgebung können Sie den Status von DB2-Datenbanken mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Systemadministrator an.
  2. Geben Sie an der Eingabeaufforderung den Befehl **su** ein, um zum Eintrag des Benutzers mit Administratorberechtigung zu wechseln, der Trust Authority installiert hat.
  3. Geben Sie das Kennwort dieses Trust Authority-Benutzers ein.
  4. Geben Sie den folgenden Befehl ein:

     ```
     set DB2INSTANCE=TrustAuthority_instance
     ```

     Hierbei steht *TrustAuthority_instance* für die ID des Benutzers, der Trust Authority installiert hat.
  5. Geben Sie für die Standard-Konfigurationsdatenbank den Befehl **db2 connect to cfgdb** ein.

     Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

     ```
     Database server = DB2/NT
     5.2.0
     SQL authorization ID = TrustAuthority_instance
     Local database alias = cfgdb
     ```
  6. Geben Sie für die Standard-CA-Datenbank den Befehl **db2 connect to ibmdb** ein.

     Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

     ```
     Database server = DB2/NT
     5.2.0
     SQL authorization ID = TrustAuthority_instance
     Local database alias = ibmdb
     ```
  7. Geben Sie für die Standard-Registrierungsdatenbank den Befehl **db2 connect to pkrfdb** ein.

Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

```
Database server = DB2/NT
5.2.0
SQL authorization ID = TrustAuthority_instance
Local database alias = pkrfdb
```

8. Geben Sie für die Standard-Prüfdatenbank den Befehl **db2 connect to adtdb** ein.

   Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

   ```
   Database server = DB2/NT
   5.2.0
   SQL authorization ID = TrustAuthority_instance
   Local database alias = adtdb
   ```

9. Kehren Sie zum Root zurück.
10. Wechseln Sie durch Eingabe des Befehls **su** zum Benutzereintrag mit Administratorberechtigung des Directory-Datenbankadministrators.
11. Angenommen, die Standard-Directory-Datenbank wurde mit dem Produkt installiert. Geben Sie den Befehl **db2 connect to ldapdb** ein.

    Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

    ```
    Database server = DB2/NT
    5.2.0
    SQL authorization ID = TrustAuthority_instance
    Local database alias = ldapdb
    ```

12. Kehren Sie zum Root zurück.

- Unter Windows NT:
  1. Melden Sie sich bei Windows NT als Systemadministrator an.
  2. Starten Sie ein DB2-Befehlsfenster.
  3. Geben Sie den folgenden Befehl ein:

     ```
     set DB2INSTANCE=TrustAuthority_instance
     ```

     Hierbei steht *TrustAuthority_instance* für die ID des Benutzers, der Trust Authority installiert hat.
  4. Geben Sie für die Standard-Konfigurationsdatenbank den Befehl **db2 connect to cfgdb** ein.

     Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

     ```
     Database server = DB2/NT
     5.2.0
     SQL authorization ID = TrustAuthority_instance
     Local database alias = cfgdb
     ```

  5. Geben Sie für die Standard-CA-Datenbank den Befehl **db2 connect to ibmdb** ein.

     Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

     ```
     Database server = DB2/NT
     5.2.0
     SQL authorization ID = TrustAuthority_instance
     Local database alias = ibmdb
     ```

  6. Geben Sie für die Standard-Registrierungsdatenbank den Befehl **db2 connect to pkrfdb** ein.

     Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

     ```
     Database server = DB2/NT
     5.2.0
     SQL authorization ID = TrustAuthority_instance
     Local database alias = pkrfdb
     ```

7. Geben Sie für die Standard-Prüfdatenbank den Befehl **db2 connect to adtdb** ein.

   Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

   ```
   Database server = DB2/NT
   5.2.0
   SQL authorization ID = TrustAuthority_instance
   Local database alias = adtdb
   ```

8. Geben Sie den folgenden Befehl ein:

   set DB2INSTANCE=*ldap_Instance*

   Hierbei steht *ldap_Instance* für ldapInst, wenn das Directory zusammen mit dem Produkt installiert wurde.

9. Angenommen, die Standard-Directory-Datenbank wurde mit dem Produkt installiert. Geben Sie den Befehl **db2 connect to ldapInst** ein.

   Bei erfolgreicher Verbindung gibt das System folgende Nachricht zurück:

   ```
   Database server = DB2/NT
   5.2.0
   SQL authorization ID = TrustAuthority_instance
   Local database alias = ldapInst
   ```

10. Schließen Sie das DB2-Befehlsfenster.

DB2-Protokolle prüfen

Die DB2-Protokolle werden von Trust Authority im Hinblick auf den Systembetrieb nicht verwendet. Weitere Informationen zu den Protokollen finden Sie in der Dokumentation zu IBM DB2.

Directory-Server verwalten

In diesem Abschnitt werden grundlegende Prozeduren für Betrieb und Verwaltung von IBM SecureWay Directory erläutert. Für einige dieser Verwaltungs-Tasks ist ein Kennwort erforderlich. Informationen zum Ändern des Kennworts für den Prüfadministrator finden Sie im Abschnitt „Trust Authority-Kennwörter ändern" auf Seite 5.

Dieser Directory-Server unterstützt LDAP-Standards (LDAP = Lightweight Directory Access Protocol). Er verfügt über eine DB2-Datenbank und befindet sich auf einer lokalen oder fernen Maschine. Bei diesem Server kann es sich um einen bereits vorhandenen oder einen speziell für Trust Authority installierten und konfigurierten Server handeln.

Weitere Informationen zur Interaktion zwischen Trust Authority und dem Directory finden Sie im Handbuch *Using the SecureWay Directory With Trust Authority*. Dieses Dokument erhalten Sie über die Seite für die Bibliothek (Library) der IBM SecureWay Trust Authority-Web-Site.

Directory-Server-Status prüfen

Je nach Umgebung können Sie den Status des Directory-Servers mit folgenden Prozeduren prüfen:

- Unter AIX:
  1. Melden Sie sich bei AIX als Root an.
  2. Prüfen Sie die Prozeßtabelle, und suchen Sie nach folgender Zeichenfolge:

     ```
     slapd
     ```

     Finden Sie diesen Prozeß, fahren Sie mit Schritt 3 fort. Finden Sie diesen Prozeß nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 120 nach.
  3. Wechseln Sie in das Verzeichnis bin. Dieses Verzeichnis hat folgenden Standardpfad:

     ```
     /usr/lpp/iau/bin
     ```
  4. Stellen Sie sicher, daß das Directory erfolgreich antwortet und verwenden Sie hierzu folgenden Befehl:

     isdirup -h *Server* **-a** *Port* **-p** *Directory_Standard_Installationspfad* **-t1**

     Hierbei steht *Server* für den Namen der Maschine, auf der das Directory ausgeführt wird und *Port* steht für den vom Directory-Server überwachten Anschluß.

     Ist die Antwort des Directory erfolgreich, wird folgende Nachricht angezeigt:

     ```
     isdirup: returning: 0
     ```
- Unter Windows NT:
  1. Melden Sie sich bei Windows NT als Systemadministrator an.
  2. Starten Sie den Task-Manager durch Drücken der Tastenkombination **Strg**, **Alt** und **Entf**.
  3. Wählen Sie die Registerkarte **Prozesse** aus.
  4. Suchen Sie nach dem Prozeß slapd.exe.

     Finden Sie diesen Prozeß, fahren Sie mit Schritt 5 fort. Finden Sie diesen Prozeß nicht, lesen Sie bitte im Abschnitt „Fehlerbehebung” auf Seite 120 nach.
  5. Wechseln Sie an der MS DOS-Eingabeaufforderung in das Verzeichnis 'bin'. Dieses Verzeichnis hat folgenden Standardpfad:

     ```
     c:\Program Files\IBM\Trust Authority\bin
     ```
  6. Stellen Sie sicher, daß das Directory erfolgreich antwortet und verwenden Sie hierzu folgenden Befehl:

     isdirup -h *Server* **-a** *Port* **-p** *Directory_Standard_Installationspfad* **-t1**

     Hierbei steht *Server* für den Namen der Maschine, auf der das Directory ausgeführt wird und *Port* steht für den vom Directory-Server überwachten Anschluß.

     Ist die Antwort des Directory erfolgreich, wird folgende Nachricht angezeigt:

     ```
     isdirup: returning: 0
     ```

Directory-Server-Protokolle prüfen

Sie können die Protokolle des Directory-Servers an den im Abschnitt Tabelle 11 beschriebenen Positionen prüfen.

Tabelle 11. Protokolle des Directory-Servers

AIX-Standardpfad	Windows NT-Standardpfad	Beschreibung
/tmp/slapd.errors	c:*Directory-Installationspfad*\tmp\slapd.errors\	Fehlerprotokoll für das Directory.

IBM SecureWay 4758 PCI Cryptographic Coprocessor verwalten

Der IBM SecureWay 4758 PCI Cryptographic Coprocessor ist eine Trust Authority-Zusatzkomponente. Der IBM SecureWay 4758 PCI Cryptographic Coprocessor ist eine programmierbare PCI-Bus-Verschlüsselungskarte mit Manipulationsschutz, die DES- und RSA-Verschlüsselungsoperationen mit hoher Geschwindigkeit ermöglicht. In Trust Authority ist die Unterstützung für 4758 nur unter AIX verfügbar.

Sie können den Status des IBM SecureWay 4758 PCI Cryptographic Coprocessor mit dem Dienstprogramm csufcnm prüfen.

Der IBM SecureWay 4758 PCI Cryptographic Coprocessor erstellt keine Protokolle. Wenn beim IBM 4758 ein Fehler auftritt, werden normalerweise ein Rückkehrcode und ein Ursachencode zusammen mit dem Fehler ausgegeben. Eine umfassende Liste mit den Rückkehr- und Ursachencodes sowie den zugehörigen Erläuterungen finden Sie im Dokument *IBM 4758 CCA Basic Services Reference and Guide*. Diese Codes sind normalerweise ausreichend für eine vorläufige Fehlerbehebung.

Die Dokumentation zum IBM SecureWay 4758 PCI Cryptographic Coprocessor enthält weitere Informationen hierzu.

Kapitel 4. Erläuterungen

Dieses Kapitel enthält Erläuterungen zur effizienten Verwaltung des Trust Authority-Systems. Die Abschnitte umfassen allgemeine Sicherheitsaspekte von Trust Authority sowie Informationen zu den Trust Authority-CAs (Zertifikatsaussteller), RAs (Registrierungsstellen) und zum Prüfsubsystem.

Trust Authority - Sicherheit

Das IBM Trust Authority-Sicherheits- und Sicherungsmodell verfügt über folgende Merkmale:

- Trust Authority verwendet Code-Unterzeichnungen, um die Software abzusichern, die Operationen auf Schlüsselbasis durchführt.
- Trust Authority verwendet KeyStores zur Speicherung von und für den Zugriff auf Identitätsnachweise für Komponenten, wie beispielsweise Schlüssel und Zertifikate. In den Komponenten-KeyStores gespeicherte Identitätsnachweise werden mit Hilfe eines Chiffrierschlüssels verschlüsselt, der von einem eingegebenen Kennwort abgeleitet wird.
- Zum Zwecke der Authentifizierung wird auch die Kommunikation zwischen Komponenten unterzeichnet. Hierzu zählen beispielsweise PKIX-Nachrichten zwischen der RA und dem CA.
- Für AIX-Systeme bietet Trust Authority Schutz von Unterschriftsschlüsseln auf der Grundlage der Hardwareeinheit IBM 4758.

Zugriffssteuerungslisten

Zugriffssteuerungslisten (ACL = Access Control Lists) bieten einen Mechanismus zur Einschränkung der Nutzung einer spezifischen Ressource auf berechtigte Benutzer. Zu den Trust Authority-Komponenten, die ACLs nutzen, zählen CA, RA und das Directory.

Der CA verwendet ACLs, um den Zugriff auf CA-Funktionen, wie beispielsweise die Erstellung von Zertifikaten, zu beschränken. Die RA verwendet ACLs, um den Zugriff auf RA-Funktionen, wie beispielsweise die Genehmigung von Anforderungen, zu beschränken. Das Directory nutzt ACLs, um den Zugriff auf verschiedene Directory-Bereiche zu begrenzen, die möglicherweise sensible Informationen enthalten.

Zertifikatsaussteller

Ein Zertifikatsaussteller (CA = Certificate Authority) ist die Entität, die für die Einhaltung der Sicherheitsregeln eines Unternehmens verantwortlich ist und sichere elektronische Identitäten in Form von Zertifikaten zuweist. Die mit dem privaten Schlüssel des CA unterzeichneten Zertifikate enthalten Identifikations- und andere Informationen zum Eigentümer des Zertifikats.

Der IBM Trust Authority-CA hat folgende Aufgaben:

- Verarbeitung von Ausstellungs-, Erneuerungs- oder Widerrufanforderungen der RAs.

- Verwaltung einer Zugriffssteuerungsliste (ACL), die durch Dateiberechtigungen geschützt ist. Diese Liste enthält die registrierten Namen (DNs) berechtigter RAs und Administratoren.
- Verwaltung einer Liste der ausgegebenen Zertifikate (ICL = Issued Certificates List) in der CA-Datenbank. Diese Liste enthält Informationen zum Zertifikatstatus, zur Seriennummer sowie CRL-Informationen.

  Der CA leitet ICL-Informationen an die Trust Authority-RA weiter, die wiederum Zertifikate und CRLs im Directory veröffentlicht.

  In der CA-Datenbank gespeicherte Sätze verwenden zum Schutz einen Nachrichtenauthentifizierungscode (MAC = Message Authentication Code). Die Prüfung dieser Sätze ist eine Trust Authority-Option mit der Bezeichnung Integritätsprüfung.
- Speicherung der eigenen Schlüssel und Zertifikate im Trust Authority-KeyStore.
- Erzeugung von Prüfsätzen für sicherheitsrelevante Ereignisse und deren Weiterleitung an den Prüf-Server.
- Unterstützung von gegenseitiger Zertifizierung und CA-Hierarchien.
- Unterstützung der Erzeugung und Bestätigung von Zertifikaten, die benutzerdefinierte und vom Benutzer ausgewählte Zertifikatserweiterungen enthalten.

CA-Hierarchien

Eine CA-Hierarchie ist eine Sicherungsstruktur, bei der sich ein CA an der Spitze dieser Struktur befindet. Dieser Spitze können bis zu vier CA-Ebenen untergeordnet sein. Werden Benutzer oder Server bei einem CA registriert, erhalten Sie ein Zertifikat, das von diesem CA unterzeichnet wurde. Auf diese Weise übernehmen Sie die Zertifizierungshierarchie der darüberliegenden Ebenen. In Trust Authority kann ein CA als Teil einer Hierarchie konfiguriert werden. In diesem Fall wird das CA-Zertifikat von einem anderen CA unterzeichnet. Der CA kann so konfiguriert werden, daß er selbstunterzeichnete Zertifikate unterstützt. In diesem Fall ist der CA nicht Bestandteil einer CA-Hierarchie.

Trust Authority unterstützt eine hierarchische Zertifizierung nur zwischen CAs, die das PKIX-CMP-Protokoll sowie die Protokolle PKCS #7 und PKCS #10 einhalten.

Zertifikatserweiterungen

X.509v3-Zertifikatserweiterungen bieten Methoden zur Zuordnung weiterer Attribute zu Benutzern oder öffentlichen Schlüsseln und zur Verwaltung der CA-Hierarchie. Das X.509v3-Format ermöglicht Benutzergemeinschaften außerdem, private oder allgemeine Erweiterungen zu definieren, die spezifische Informationen für diese Gemeinschaft enthalten.

Jede Erweiterung eines Zertifikats kann als kritisch oder unkritisch gekennzeichnet werden. Ein System, das Zertifikate im X.509v3-Format nutzt, muß ein Zertifikat zurückweisen, wenn dieses eine kritische Erweiterung enthält, die dem System nicht bekannt ist. Eine unbekannte unkritische Erweiterung kann jedoch ignoriert werden.

Es gibt drei Arten von Zertifikatserweiterungen:

- Standarderweiterungen
- Allgemeine Erweiterungen
- Private Erweiterungen

Standarderweiterungen

Eine Zertifikatsstandarderweiterung ist eine Erweiterung, deren Bedeutung und Syntax im ITU-Standard RFC 2459 definiert ist. Bis auf eine sind alle diese Erweiterungen auch in X.509v3 definiert. Einige von ihnen sind nur innerhalb von CA-Zertifikaten definiert. Trust Authority ermöglicht das Hinzufügen der meisten Standarderweiterungen zu einem Zertifikat (hierfür gelten die im Abschnitt Tabelle 12 beschriebenen Regeln):

Tabelle 12. Zertifikatserweiterungen

Erweiterung	Beschreibung
Schlüsselverwendung	Diese Erweiterung gibt den Zweck der Verwendung des zertifizierten öffentlichen Schlüssels an. Die Einstellungen werden in der Regel durch Zertifizierungsschablonen definiert.
Alternativer Name des Zertifikatsgegenstands	Diese Erweiterung enthält einen oder mehrere Alternativnamen in verschiedenen Namensformaten für die Entität, die vom CA dem zertifizierten öffentlichen Schlüssel zugeordnet wurde. In der Regel wird in Zertifizierungsschablonen definiert, welche dieser Namensformate in Zertifikaten verwendet werden dürfen, die diese Schablone nutzen.
Schlüsselkennung des Zertifikatsgegenstands	Diese Erweiterung legt fest, welcher öffentliche Schlüssel durch ein bestimmtes Zertifikat zertifiziert wird. Diese Erweiterung dient primär der Unterscheidung von Schlüsseln, wenn mehrere Schlüssel für eine Entität zertifiziert sind oder zertifiziert wurden. Der Wert dieser Erweiterung wird in Trust Authority immer vom CA definiert.
Schlüsselkennung des Ausstellers	Diese Erweiterung gibt an, welcher öffentliche Schlüssel vom Aussteller eines Zertifikats zu dessen Unterzeichnung verwendet wurde. Diese Erweiterung dient primär der Unterscheidung von Schlüsseln, wenn mehrere Schlüssel für einen Aussteller zertifiziert werden. Der Wert dieser Erweiterung wird immer vom CA definiert.
Nutzungszeitraum für privaten Schlüssel	Diese Erweiterung schränkt die Nutzung des privaten Schlüssels gemäß der Gültigkeitsdauer des Zertifikats ein. Das aktuelle PKIX-Zertifikatsprofil RFC 2459 gibt an, daß die Nutzung dieses Schlüssels nicht länger empfohlen wird.
Erweiterung für Zertifizierungsregeln	Diese Erweiterung enthält eine Reihe von Regelanzeigern. Ein solcher Anzeiger kann beispielsweise eine Objektkennung sein, deren Bedeutung veröffentlicht werden muß. Es kann sich jedoch auch um eine Objektkennung in Verbindung mit einer Beschreibung der angestrebten Regel handeln. Anstelle der Beschreibung kann eine URL-Adresse eingesetzt werden, unter der die Beschreibung abgerufen werden kann. Sie können jedoch auch einen kurzen Text in das Zertifikat aufnehmen.
Alternativname des Ausstellers	Diese Erweiterung enthält einen oder mehrere Alternativnamen in verschiedenen Namensformaten für den Aussteller des Zertifikats. Der Wert dieser Erweiterung wird immer vom CA definiert.

Tabelle 12. Zertifikatserweiterungen (Forts.)

Erweiterung	Beschreibung
Directory-Attribute des Zertifikatsgegenstands	Diese Erweiterung enthält eine Reihe zusätzlicher Directory-Attribute des Zertifikatsgegenstands, die nicht Teil des registrierten Namens sind. Diese Erweiterung muß als unkritisch definiert werden.
Erweiterte Schlüsselverwendung	Diese Erweiterung enthält eine Reihe von Objektkennungen, die den Nutzungszweck für den zertifizierten öffentlichen Schlüssel angeben. Die Einstellungen werden in der Regel durch Zertifizierungsschablonen definiert. Die Werte dieser Erweiterung können durch eine Benutzergemeinschaft definiert oder von RFC 2459 abgeleitet werden.
Grundlegende Einschränkungen	Diese Erweiterung ist nur bei CA-Zertifikaten sinnvoll. Sie ist in allen CA-Zertifikaten enthalten, die von Trust Authority erstellt wurden. Bei allen anderen Zertifikaten ist diese Erweiterung entweder nicht vorhanden oder leer. RFC 2459 empfiehlt, diese Erweiterung nicht leer- sondern wegzulassen. Diese Erweiterung kennzeichnet ein Zertifikat nicht nur als CA-Zertifikat, sondern kann auch den Zertifizierungspfad mit maximaler Länge enthalten. Auf diese Weise kann definiert werden, wie viele zusätzliche CA-Ebenen durch diesen CA zertifiziert werden können. Diese Erweiterung muß als kritisch definiert werden.
Namenseinschränkungen	Diese Erweiterung wird nur in CA-Zertifikaten verwendet. Sie definiert einen Namensbereich, in dem sich alle Namen und Alternativnamen des Zertifikatsgegenstands befinden müssen, sofern es sich um Zertifikate handelt, die vom CA mit diesem Zertifikat oder von untergeordneten CAs ausgestellt wurden. Der Zweck dieser Erweiterung ist die Einschränkung von Namen, die von Zertifikaten in diesem Zertifizierungspfad genutzt werden können. Einschränkungen werden in Form von Unterverzeichnisstrukturen für zulässige oder nicht zulässige Namen definiert. Ein Name, der einer Beschränkung in einer Unterverzeichnisstruktur nicht zulässiger Namen entspricht, ist ungültig, unabhängig von den Informationen in der Unterverzeichnisstruktur der zulässigen Namen. Diese Erweiterung muß als kritisch definiert werden.
Regelzuordnung	Diese Erweiterung wird nur in CA-Zertifikaten verwendet. Trust Authority definiert diese Erweiterung nicht in Zertifikaten, für die es die ursprüngliche Anforderung erstellt hat.
Regeleinschränkungen	Diese nur in CA-Zertifikaten verwendete Erweiterung kann für einen der folgenden Zwecke eingesetzt werden: Sie kann das Zuordnen von Regeln in Zertifikaten des aktuellen Zertifizierungspfads verhindern oder für diese Zertifikate spezifische Regeln erforderlich machen.

Tabelle 12. Zertifikatserweiterungen (Forts.)

Erweiterung	Beschreibung
CRL-Verteilungspunkte	Diese Erweiterung gibt an, wo sich eine partielle CRL mit Widerrufinformationen zum aktuellen Zertifikat befindet. Sie wird gesetzt, wenn ein gültiger Wert ungleich Null für den Parameter 'certPerDP' in der Datei 'jonahca.ini' angegeben wird.
Informationszugriff für Aussteller	Diese Erweiterung gibt an, wo und wie auf bestimmte Informationen zum Aussteller des Zertifikats mit dieser Erweiterung zugegriffen werden kann. Diese Erweiterung ist derzeit in von Trust Authority erstellten Zertifikaten nicht definiert.

Allgemeine Erweiterungen

Trust Authority definiert eine einzelne, vom Standard abweichende Erweiterung als allgemeine Erweiterung. Diese Erweiterung kann von jedem Unternehmen eingesetzt werden, die Trust Authority nutzt. Es handelt sich hierbei um die Erweiterung für die Zuordnung der Host-Identität, die den Zertifikatsgegenstand einer entsprechenden Identität auf einem Host-System zuweist.

Private Erweiterungen

Jede für die Nutzung von Trust Authority ausgelegte Client-Anwendung kann eine Erweiterung definieren, deren Identität und Syntax entweder der Anwendung privat zur Verfügung stehen oder in einer Benutzergemeinschaft gemeinsam genutzt werden. Diese Erweiterungen müssen als unkritisch definiert werden. Wird die Erweiterung zum ersten Mal definiert, muß ihr eine Objektkennung zugewiesen werden. Außerdem müssen Sie sie gemäß ITU-Standard X.660 und ISO-Standard 9834-1 (identisch) registrieren. Dies gilt auch für die Syntax.

Ablauf der Erweiterungsanforderung

Erweiterungen können von einem Benutzer angefordert werden, Sie müssen jedoch vom CA oder einer RA, die als CA dient, bestätigt werden. Dieser Prozeß läuft wie folgt ab:

1. Der Benutzer fordert eine Erweiterung an und übermittelt die dazu erforderlichen Informationen, einschließlich einer eindeutigen Erweiterungskennung und eines Werts. Der Benutzer definiert die Erweiterung als kritisch oder unkritisch.
2. Die Erweiterungsanforderung und die Informationen werden in die Zertifikatsanforderung an die RA aufgenommen.
3. RA oder CA prüfen bei der Verarbeitung der Zertifikatsanforderung, ob die Erweiterung den Zertifizierungsregeln der Unternehmen entspricht. Die Erweiterungsanforderung wird dementsprechend geändert oder außer Kraft gesetzt. Nach Prüfung der Erweiterung wird diese vom CA zertifiziert.

Zertifikatwiderrufslisten

Eine Zertifikatswiderrufsliste (CRL) ist eine digital unterzeichnete, mit Zeitmarken versehene Liste der Zertifikate, die vom Zertifikatsaussteller (CA) widerrufen wurden. Die Zertifikate in dieser Liste sollten als nicht akzeptierbar behandelt werden.

Zertifikate können widerrufen werden, wenn ihre Gültigkeit abgelaufen oder ihre Sicherheit fraglich ist. Der Status eines Zertifikats wird in der ICL geändert. Zur festgelegten Zeit erstellt der CA die CRL mit der Seriennummer und dem CA-DN des Ausstellers des widerrufenen Zertifikats. Obwohl bei einem Widerruf das

entsprechende Zertifikat und dessen Informationen in der ICL geändert werden, ist ein Widerruf erst dann endgültig, wenn die CRL ausgegeben und im Directory veröffentlicht wird.

In Trust Authority werden die Gültigkeitsdauer einer veröffentlichten CRL und der Zeitraum zwischen CRL-Veröffentlichungen in der CA-Konfigurationsdatei jonahca.ini definiert und geändert.

Sie können auch CRL-Verteilungspunkte nutzen, um die Anzahl der CRLs, die nacheinander verarbeitet werden sollen, zu definieren und zu partitionieren. Statt eine immer größere Anzahl widerrufener Zertifikate an einer Position bzw. unter einem einzelnen Eintrag im Directory-Server zu akkumulieren, können Sie die Liste der widerrufenen Zertifikate auf mehrere Verteilungspunkte aufteilen. Sie aktivieren diese Funktion, indem Sie den Parameter 'certPerDp' in der Konfigurationsdatei 'jonahca.ini' entsprechend einstellen.

Gegenseitige Zertifizierung

Bei der gegenseitigen Zertifizierung handelt es sich um ein Sicherungsmodell, in dem ein Zertifikat, das einen öffentlichen CA-Schlüssel enthält, der einem entsprechenden privaten CA-Unterschriftsschlüssel für das Ausstellen von Zertifikaten zugeordnet ist, von einem CA an einen anderen CA ausgestellt wird. Typischerweise wird die gegenseitige Zertifizierung eingesetzt, um Client-Systemen oder Endentitäten in einer Registrierungsdomäne die sichere Kommunikation mit Client-Systemen oder Endentitäten in einer anderen Registrierungsdomäne zu ermöglichen.

Obwohl die gegenseitige Zertifizierung zwischen CAs in beiden Richtungen erfolgen kann, werden in Trust Authority Anforderungen für die gegenseitige Zertifizierung nur in einer Richtung unterstützt. Die gegenseitige Zertifizierung in beiden Richtungen ist möglich, wenn jeder CA ein gegenseitiges Zertifikat vom jeweils anderen CA erhält. Trust Authority unterstützt eine gegenseitige Zertifizierung nur zwischen CAs, die das PKIX-CMP-Protokoll einhalten.

Zertifizierung

Als Zertifizierung bezeichnet man die Erstellung eines digitalen Zertifikats für eine Entität oder eine Person. In Trust Authority erfolgt die Zertifizierung nur nach Prüfung und Bestätigung einer Zertifizierungsanforderung durch die RA. Als Ergebnis der Registrierung stellt der CA die entsprechenden Zertifikate aus.

Digitale Zertifikate

Ein digitales Zertifikat ist ein elektronischer Identitätsnachweis, der einer Person oder einer Entität von einer gesicherten dritten Partei ausgestellt wird. Jedes Zertifikat ist mit dem privaten Schlüssel des CA unterzeichnet. Es bürgt für die Identität einer Person, eines Unternehmens oder einer Organisation.

Abhängig vom Aufgabenbereich des CA kann das Zertifikat den Identitätsnachweis seines Inhabers bestätigen, e-Business über das Internet ausführen zu dürfen. In gewissem Sinne entspricht ein digitales Zertifikat einem Führerschein oder einem medizinischen Diplom. Es bestätigt, daß der Inhaber des entsprechenden privaten Schlüssels berechtigt ist, bestimmte e-Business-Aktivitäten auszuführen.

Ein Zertifikat enthält Informationen über die Entität, die von ihm zertifiziert wird, gibt an, ob es sich um eine Person, eine Maschine oder ein Computerprogramm handelt, und enthält als Teil dieser Informationen den zertifizierten öffentlichen Schlüssel dieser Entität.

Bei Trust Authority entspricht der Typ des ausgestellten Zertifikats den geschäftlichen Regeln Ihres Unternehmens.

Registrierte Namen

Ein registrierter Name (DN = Distinguished Name) ist der eindeutige Name eines im Directory gespeicherten Datensatzes. Der DN kennzeichnet eindeutig die Position eines Datensatzes in der hierarchischen Struktur des Directory. Diese Struktur wird auch als Directory Information Tree (DIT) bezeichnet.

Die Struktur verfügt über einen einzigen Stamm und eine unbegrenzte Anzahl von Knoten, die sich vom Stamm verzweigen. Jeder Knoten entspricht einem durch Attribute gekennzeichneten Directory-Eintrag. Die Beschreibung eines DNs für einen Directory-Eintrag hängt von den Syntaxanforderungen des Directory-Clients und dem Zugriffsprotokoll des Directory-Servers ab.

In Trust Authority, das auf IBM SecureWay Directory basiert, kann ein DN für einen Directory-Eintrag wie folgt aussehen:

```
/C=US/O=IBM/OU=Trust Authority/MAIL=cjsmith@vnet.ibm.com,CN=Chris Smith
```

Hierbei steht US für das Land (C), IBM für das Unternehmen (O), Trust Authority für die Abteilung innerhalb des Unternehmens (OU), cjsmith@vnet.ibm.com für die E-Mail-Adresse (MAIL) und Chris Smith für den allgemeinen Namen (CN).

Liste der ausgestellten Zertifikate (CRL)

Die Liste der ausgestellten Zertifikate (ICL = Issued Certificates List) ist eine vollständige Liste der Zertifikate (einschließlich deren Status), die von einem CA ausgestellt wurden. Die Zertifikate sind nach Seriennummer und Status indexiert. Die ICL wird vom CA verwaltet und in der CA-Datenbank gespeichert. Diese Liste dient zur Ermittlung der Zertifikate, die in einer Zertifikatwiderrufsliste (CRL = Certificate Revocation List) veröffentlicht werden sollten. Die Trust Authority-ICL verfügt über folgende Merkmale:

- ODBC-Implementierung (Open Database Connectivity, in Trust Authority über DB2)
- Wahlfreie Verwendung von MACs in Datenbankeinträgen zur Gewährleistung der Integrität (nur ODBC)
- Verschleierung von Chiffrier- und MAC-Schlüssel zur Laufzeit
- Unterstützung mehrerer Verbindungen (pro Thread) mit einem standardmäßigen Maximalwert
- Zugriff auf die Prüfprotokollfunktion

Unterzeichnen und Gültigkeitsprüfung für Unterschriften

Unterzeichnen bedeutet, eine Unterschrift mit Hilfe eines privaten digitalen Schlüssels zu erstellen. Eine Gültigkeitsprüfung beinhaltet die Verwendung des entsprechenden öffentlichen Schlüssels zur Bestätigung der Unterschrift.

Trust Authority verwendet zur Unterzeichnung und für Gültigkeitsprüfungen eine Verschlüsselungsmaschine auf PKIX-Basis. Dieses Produkt ermöglicht es Anwendungen, Informationen zu ver- und entschlüsseln. Mit diesem Produkt können

Anwendungen eine digitale Unterschrift prüfen, ein Zertifikat von einem Directory abrufen und entscheiden, ob ein Zertifikat gesichert ist. Diese Verschlüsselungsmaschine bietet außerdem nahtlose Unterstützung für die hardwaregestützte Verschlüsselung. Sie unterstützt den IBM SecureWay 4758 PCI Cryptographic Coprocessor oder jedes andere Hardware-Token mit PKCS #11-Schnittstelle.

Alle Trust Authority-Softwarekomponenten, die Verschlüsselungs- und KeyStore-Operationen durchführen, werden von dieser Verschlüsselungsmaschine unterzeichnet.

Registrierungsstellen (RA)

Eine Registrierungsstelle (RA = Registration Authority) ist ein Server-Prozeß, der die administrativen Aufgaben im Bereich der digitalen Zertifizierung übernimmt. In Trust Authority kann eine RA Anforderungen genehmigen oder zurückweisen sowie den Widerruf eines Zertifikats einleiten. Die RA gewährleistet, daß die geschäftlichen und Zertifizierungsregeln eines Unternehmens eingehalten werden.

Registratoren

Registratoren können über den Trust Authority RA Desktop administrative Tasks für Registrierungsanforderungen ausführen. Damit ein Registrator diese Tasks ausführen kann, müssen Sie ihn als Registrator registrieren. Nähere Informationen hierzu finden Sie im Abschnitt „Einen Registrator hinzufügen" auf Seite 35.

Über den RA Desktop können Registratoren folgende Statuswerte von Zertifikatsanforderungen abrufen: Empfangen, Anstehend, Genehmigt, Nicht genehmigt, Abgeschlossen. Zu den weiteren Abfragefeldern des RA Desktop zählen Vor- und Nachname, Aktualisierungsdatum, Erstellungsdatum und Ablaufdatum des Zertifikats. Zeigt der RA Desktop die zu einer Abfrage gefundenen Einträge in Tabellenform an, kann der Registrator für die Ergebnisse weitere Maßnahmen ergreifen. So kann er beispielsweise eine Registrierungsanforderung bestätigen oder zurückweisen oder den Erneuerungsstatus eines Zertifikats widerrufen oder ändern.

Registrierungsdomänen

Eine Registrierungsdomäne ist eine Gruppe von Ressourcen, Regeln und Konfigurationsoptionen, die sich auf bestimmte Registrierungsprozesse für Zertifikate beziehen. Der Domänenname ist eine Untergruppe der URL-Adresse, die zum Widerrufen von Registrierungsoperationen verwendet wird. Sie dient als eindeutige Unterzeichnung der Anwendung. Trust Authority unterstützt eine Registrierungsdomäne pro Trust Authority-Installation.

IBM SecureWay 4758 PCI Cryptographic Coprocessor

Der IBM SecureWay 4758 PCI Cryptographic Coprocessor ist eine programmierbare PCI-Bus-Verschlüsselungskarte mit Manipulationsschutz, die zur Gewährleistung der Vertraulichkeit und Integrität des Unterschriftsschlüssels Ihres Unternehmens beiträgt. Diese Karte verwendet die API der IBM Common Cryptographic Architecture (CCA) und stellt umfassende Verschlüsselungsservices, einschließlich DES- und RSA-Verschlüsselung, zur Verfügung. DES und RSA sind die am weitesten verbreiteten Algorithmen für kommerzielle Verschlüsselungssysteme. Aufgrund der Leistungsfähigkeit dieser Algorithmen sollten Sie den von Ihnen verwendeten Methoden zur Schlüsselverwaltung besondere Aufmerksamkeit zukommen lassen. Ist die Vertraulichkeit eines Schlüssels nicht mehr gewährleistet, können unter Umständen Unbefugte auf die mit diesem Schlüssel verschlüsselten

Daten zugreifen. Der IBM SecureWay 4758 PCI Cryptographic Coprocessor ermöglicht mit folgenden Merkmalen die Erweiterung des umfassenden Schutzes für diese Schlüssel:

- Dreifache Verschlüsselung von Schlüsseln mit Hilfe eines speziellen, in der dedizierten Hardware gespeicherten Schlüssels
- Schutz von Endpunkt-zu-Endpunkt-Datenübertragungen
- Programmatisches Definieren von änderbaren Regeln und Profilen
- Nutzung eines Zufallsgenerators auf Hardwarebasis zur Erstellung nicht vorausberechenbarer Schlüssel

Die Verschlüsselungsprozesse finden in einem sicheren und abgegrenzten Bereich auf der Karte statt. Die Karte ist so ausgelegt, daß sie den strengen Anforderungen des Standards FIPS PUB 140-1 Stufe 4 entspricht. Innerhalb des sicheren Bereichs kann Software ausgeführt werden.

In Trust Authority ermöglicht der IBM SecureWay 4758 PCI Cryptographic Coprocessor die Erstellung von CA-Unterschriftsschlüsseln. Die durch den IBM SecureWay 4758 PCI Cryptographic Coprocessor erstellten Schlüssel werden von der Karte geschützt, indem sie mit dem in die Karte integrierten Hauptschlüssel verschlüsselt werden. Die CA-Schlüssel können entweder im KeyStore oder im IBM SecureWay 4758 PCI Cryptographic Coprocessor gespeichert werden.

Der IBM SecureWay 4758 PCI Cryptographic Coprocessor ist eine wahlfreie, aber empfohlene Trust Authority-Komponente, die nur für die AIX-Plattform verfügbar ist.

Smart Cards

Smart Cards sind mobile Verschlüsselungseinheiten in der Größe einer Kreditkarte. Sie werden sowohl zur Speicherung von Zertifikaten und Schlüsseln als auch für Verschlüsselungsoperationen (beispielsweise Unterschriften) eingesetzt. Hierbei verläßt der private Schlüssel die Karte nicht. Nicht alle Benutzer können auf Smart Card-Hardware zugreifen. Daher bietet Trust Authority eine virtuelle Smart Card, die sich wie eine reale Smart Card verhält.

Benutzer von Trust Authority-Clients können Zertifikate auf virtuellen und realen Smart Cards speichern. Übergibt der Benutzer einer Trust Authority-Client-Anwendung eine Zertifikatsanforderung, wird ein privater Schlüssel auf dessen virtueller oder realer Smart Card gespeichert. Nach der Bestätigung wird das Zertifikat an den Benutzer zurückgegeben. Alle auf der Smart Card gespeicherten Zertifikate können einem privaten Schlüssel zugeordnet werden, indem die Kennung des gespeicherten privaten Schlüssels verwendet wird.

CA und RA speichern jeweils einen privaten Schlüssel und die entsprechenden selbstunterzeichneten Zertifikate auf ihren Smart Cards. Auf diese Weise kann die RA Nachrichten und der CA CRLs und Zertifikate unterzeichnen, ohne daß ihre privaten Schlüssel die Smart Cards verlassen.

Trust Authority implementiert die PKCS #11-Schnittstelle für Smart Card-Speichereinheiten.

Prüfung

Das Trust Authority-Prüfsubsystem bietet Unterstützung für die Protokollierung sicherheitsrelevanter Aktionen auf der Grundlage der Empfehlungen des Standards X9.57 für den Finanzsektor. Auf diese Weise können Sie Prüfprotokolle verwalten und archivieren und Integritätsprüfungen von Protokolleinträgen durchführen.

Das Prüfsubsystem besteht aus einer Client-Bibliothek und einem Prüf-Server. Der Prüf-Server empfängt Prüfereignisse von autorisierten Clients und schreibt diese Ereignisse in ein integritätsgeschütztes Prüfprotokoll. Alle Protokolleinträge werden in einer DB2-Datenbank gespeichert. Prüfereignisse werden außerdem in einer Datei gespeichert. Abfrage- und Berichterstellungs-Tools werden von DB2 UDB bereitgestellt.

Protokolleinträge

Protokolleinträge werden in Form eines Prüfprotokolls in einer DB2-Datenbank gespeichert. Das Prüfprotokoll enthält pro Prüfereignis einen Protokolleintrag. Die Prüfdatenbank hilft bei der Manipulationserkennung, wie im Standard für den Finanzsektor X9.57 vorgeschrieben. Jeder Protokolleintrag ist durch eine Seriennummer eindeutig gekennzeichnet.

Prüfereignisse

Trust Authority-Prüfereignisse sind Sätze, die die Bedeutung einer sicherheitsrelevanten Task angeben. Der Prüf-Server empfängt Prüfereignisse von autorisierten Clients und schreibt diese Ereignisse in ein integritätsgeschütztes Prüfprotokoll.

Trust Authority-Prüfereignisse werden in folgende Kategorien unterteilt:

- Schlüsselverwaltungsereignisse

  Ereignisse im Zusammenhang mit der sicheren Verwaltung von Schlüsseln, um Benutzern Schlüssel am gewünschten Ort und zur gewünschten Zeit bereitstellen zu können.
- Zertifikatsverwaltungsereignisse

  Ereignisse, die sich aus der Verwaltung digitaler Zertifikate und aus der Pflege von Informationen zu Zertifikaten und CRLs im Directory ergeben.
- Sicherheitsrelevante Ereignisse

  Ereignisse, die sich aus der Ausführung sicherheitsrelevanter Tasks ergeben. Hierzu zählen beispielsweise Integritätsprüfungen, Authentifizierungen und Zertifikatsprüfungen.
- Ereignisse für Prüfadministratoren

  Diese Ereignisse ergeben sich aus Aktionen, die mit den Aufgaben von Prüfadministratoren zusammenhängen. Die Aufgaben eines Prüfadministrators umfassen die Implementierung der Sicherheitsregeln Ihres Unternehmens.
- RA-Ereignisse

  Ereignisse, die sich aus den Aktionen einer RA ergeben.

Nähere Informationen zu Prüfereignissen finden Sie im Abschnitt „Felder für Prüfereignisse” auf Seite 109.

Masken für Prüfereignisse

In Trust Authority bieten Masken für Prüfereignisse Unterstützung für die Steuerung der Prüfereignisse, die an den Prüf-Server weitergeleitet werden. Beachten Sie, daß eine verbindliche Untermenge von Prüfereignissen nicht von Maskenspezifikationen beeinflußt wird.

Informationen zum Definieren einer Maske für Prüfereignisse finden Sie im Abschnitt „Prüfmaske definieren" auf Seite 47.

Verbindliche und wahlfreie Prüfereignisse

Eine bestimmte Untermenge von Prüfereignissen ist verbindlich. Diese Ereignisse werden von Maskendefinitionen in der Konfigurationsdatei des Prüf-Clients nicht betroffen. Informationen zu verbindlichen und wahlfreien Prüfereignissen finden Sie in Tabelle 19 auf Seite 110.

Integritätsprüfung

Trust Authority bietet ein Tool, mit dem geprüft werden kann, ob Prüfsätze unberechtigterweise verändert wurden. Dieses Tool trägt die Bezeichnung Audit Integrity Check. Integritätsprüfungen unterscheiden sich von Maßnahmen zum Schutz der Vertraulichkeit von Daten zum Zwecke der Geheimhaltung.

Der Prüf-Server unterzeichnet nicht jeden Eintrag. Statt dessen wendet er auf jeden Eintrag einen Nachrichtenauthentifizierungscode (MAC = Message Authentication Code) an und verwaltet einen MAC für die gesamte Datenbank.

Integritätsversiegelung

In Trust Authority bedeutet Integritätsversiegelung das Unterzeichnen archivierter Datenbankdateien mit Prüfprotokollen. Das Unterzeichnen erfolgt mit Hilfe des Trust Authority-Befehlszeilen-Tools Audit Archive and Sign.

Archivieren von Prüfprotokollen

Trust Authority unterstützt das Archivieren des aktuellen Prüfprotokolls in eine Archivdatei. Hierzu wird das Befehlszeilen-Tool Audit Archive and Sign verwendet.

DB2-Datenbanken

IBM DB2 Universal Database (DB2 UDB) ist ein web-fähiges Verwaltungssystem für relationale Datenbanken mit Java-Unterstützung. In Trust Authority können mit IBM DB2 Universal Database folgende Tasks ausgeführt werden:

- Verwalten von Informationen zu Registrierungsprozessen für digitale Zertifikate.
- Speichern von Informationen zu RA-Aktionen, mit denen Anforderungen für digitale Zertifikate genehmigt oder zurückgewiesen werden. Diese Informationen werden zu Prüfungszwecken verwendet.
- Bereitstellen von Betriebsstatistiken zur Gesamtauslastung der Trust Authority-Registrierungsfunktion.
- Bereitstellen von Datenbanken für den Trust Authority-CA, die RA, das Prüfsubsystem, das Directory und die Trust Authority-Konfigurationsdaten.

Web-Server

Web-Server sind Server-Programme, die auf Informationsanforderungen von Browsern reagieren. Trust Authority verwendet IBM WebSphere-Softwareprodukte, um eine gesicherte Grundlage für solche Netztransaktionen bereitzustellen. Der WebSphere Application Server und der IBM HTTP Server stellen in Trust Authority die Infrastruktur für Web-Server-Funktionalität zur Verfügung.

In einem Trust Authority-System befindet sich die Web-Server-Software auf der gleichen Maschine wie die RA. Sie ermöglicht eine sichere Abgrenzung zwischen geschützten Programmen und den Benutzern, die auf diese Programme zugreifen wollen. Mit Hilfe der HTTP- und HTTPS- (Hypertext Transfer Protocols) sowie der SSL-Technologie (Secure Sockets Layer) kann das Web-Server-Produkt die Kommunikation zwischen Client und Server verschlüsseln. Darüber hinaus können Client-Authentifizierungen durchgeführt werden, um unbefugten Zugriff oder Datenmanipulationen zu verhindern.

IBM WebSphere Application Server

Der IBM WebSphere Application Server (WAS) ist ein Server für Java-Anwendungen, der die Verwaltung und Nutzung von Web-Anwendungen vereinfachen soll. WAS muß auf einem Host-Web-Server installiert sein, der HTTP-Anforderungen von Browsern verarbeitet und die Antworten über das HTTP-Protokoll im HTML-Format zurückgibt. Bei der Installation von WebSphere wird die Konfiguration des entsprechenden Host-Web-Servers so verändert, daß bestimmte Anforderungen zur Verarbeitung an WebSphere und nicht an den Web-Server weitergeleitet werden. WAS nutzt eine Java-Entwicklungs- und -Laufzeitumgebung auf der Host-Maschine. Diese Java-Umgebung ermöglicht WebSphere die Ausführung von Java-Programmen, die von der Trust Authority-Registrierungsfunktion verwendet werden.

IBM HTTP Server

Der Trust Authority-Server basiert auf einem Modell mit drei Servern und drei Anschlüssen, um die Client-Anforderungen zu verarbeiten. Ihr Unternehmen hat sich möglicherweise für die Installation eines einzigen Exemplars des IBM HTTP Server und für die Konfiguration verschiedener virtueller Host-Namen und Anschlüsse entschieden, um verschiedene Arten von Anforderungen verarbeiten zu können.

Mit diesem Modell verarbeitet Trust Authority folgende Arten von Anforderungen:

- Anforderungen, die keine Verschlüsselung oder Authentifizierung benötigen.
- Anforderungen, die Verschlüsselung und Server-Authentifizierung benötigen.
- Anforderungen, die Verschlüsselung sowie Server- und Client-Authentifizierung benötigen.

Im Abschnitt Tabelle 13 werden diese Konfigurationsalternativen erläutert.

Tabelle 13. Modell für IBM HTTP Server mit drei Servern und drei Anschlüssen

Protokoll	SSL	Server-Authentifizierung	Client-Authentifizierung	Beispiel für Anschlußnummer bei einer IP	Beispiel für Anschlußnummer bei mehreren IPs
HTTP	Nein	Nein	Nein	80	80
HTTPS	Ja	Ja	Nein	443	443
HTTPS	Ja	Ja	Ja	1443	443

IP-Aliasing

Im Bereich der Internet-Technologie ist ein Aliasname ein Name, der einem Server zugeordnet wird, so daß der Server vom Namen seiner Host-Maschine unabhängig wird. Der Aliasname muß im Domain Name System (DNS) Ihres Systems definiert werden.

Directory-Server

Trust Authority verwendet das IBM SecureWay Directory zur Speicherung von digitalen X.509-Zertifikaten, Zertifikatswiderrufslisten (CRLs), CA-Regeln und weiterer Informationen zu registrierten Servern und Benutzern. Mit dieser Komponente kann nach einem Zertifikat für einen öffentlichen Schlüssel einer bestimmten Person oder eines Servers gesucht werden. Hierzu wird das Directory nach dem eindeutigen registrierten Namen (DN) der Person oder des Servers oder nach anderen relevanten Informationsquellen durchsucht.

Dieser Server unterstützt LDAP-Standards (LDAP = Lightweight Directory Access Protocol) und basiert auf DB2 UDB. Er wird als eigenständiger Dämon ausgeführt und verwendet ein Client/Server-Modell, um Trust Authority den Zugriff auf den Server zu ermöglichen. Der Server nutzt eine Schnittstelle auf Web-Basis, um das Directory einzurichten, zu verwalten und die enthaltenen Daten anzuzeigen. Als Directory kann ein vorhandener Server oder ein speziell für Trust Authority installierter und konfigurierter Server dienen. Nähere Informationen hierzu finden Sie im Abschnitt *Using the SecureWay Directory With Trust Authority* auf der folgenden Web-Site von IBM SecureWay Trust Authority:

`http://www.tivoli.com/support`

Objektkennungen

Eine Objektkennung (OID = Object Identifier) ist ein Wert, der sich von allen ähnlichen Werten unterscheidet und der einem Objekt zugeordnet ist. Jede gemäß ASN.1 definierte OID bildet einen Knoten einer Baumstruktur (ähnlich wie bei DIT). Eine Objektkennungsbaumstruktur ist eine Baumstruktur, deren Stamm den ITU-Empfehlungen X.680 entspricht. Die Scheitelpunkte entsprechen Administratorberechtigungen für die Zuordnung von Bögen (Segmenten, die zwei Scheitelpunkte verbinden) von diesem Scheitelpunkt (ein Punkt, der sich am Ende eines Bogens oder am Schnittpunkt von Bögen befinden kann).

Jeder Bogen in der Baumstruktur ist durch eine Objektkennungskomponente (ein numerischer Wert) gekennzeichnet. Jedes zu unterzeichnende Objekt ist genau einem Scheitelpunkt (in der Regel ein Blatt des Baums) zugeordnet. Kein anderes Objekt (der gleichen oder einer anderen Art) wird diesem Scheitelpunkt zugeordnet. Aus diesem Grund wird ein Objekt eindeutig durch die Reihenfolge der numerischen Werte (Objektkennungskomponenten) der Bögen vom Stamm bis zum Scheitelpunkt des Objekts unterzeichnet.

Direkt unterhalb des Stamms werden derzeit drei Werte definiert. Sie lauten 0, 1 und 2:

- 0 wird CCITT-Empfehlungen zugewiesen.
- 1 wird ISO-Empfehlungen zugewiesen.
- 2 wird beiden Unternehmen gemeinsam zugewiesen.

So fallen beispielsweise alle OIDs, die für den Directory-Standard definiert sind, unter die gemeinsame CCITT/ISO-Kategorie 2 und werden der Objektkennungskomponente 5 zugeordnet. Aus diesem Grund beginnen alle OIDs für Directory-Standardobjekte mit dem Präfix 2.5.

Kapitel 5. Referenzinformationen

Dieses Kapitel enthält Referenzinformationen zu folgenden Themen:

- Konfigurationsdateien

  Informationen zu Parameternamen, Beschreibungen und Formaten. Es wird angegeben, ob die Parameter verbindlich oder wahlfrei sind und ob sie konfiguriert werden können.
- Befehle

  Syntax- und Parameterbeschreibungen für die Trust Authority-Befehlszeilendienstprogramme.
- Felder für Prüfereignisse

  Dieser Abschnitt erläutert die Informationen, die in Trust Authority-Prüfereignissen enthalten sind.
- Prüfereignisse

  Dieser Abschnitt erläutert Prüfereignisse und gibt an, ob ein Ereignis verbindlich oder wahlfrei ist.
- Daten in der Prüfdatenbank

  Dieser Abschnitt beschreibt die Speicherung von Protokolleinträgen in den Tabellen der relationalen Datenbank. Hier finden Sie Informationen zu den Feldnamen im Datensatz (bzw. den Spaltennamen in der Tabelle), zu den Speicherorten der Daten sowie Beschreibungen der Felder und der Datenformate.
- Fehlerbehebung

  Dieser Abschnitt enthält Informationen zur grundlegenden Fehlerbehebung sowie zur Nachrichtenerstellung auf Debug-Stufe.

Konfigurationsdateien

Dieser Abschnitt enthält die Beschreibungen der Parameter für folgende Konfigurationsdateien:

- CA-Server-Konfigurationsdatei jonahca.ini
- RA-Server-Konfigurationsdatei jonahra.ini
- Prüf-Server-Konfigurationsdatei AuditServer.ini
- Prüf-Client-Konfigurationsdatei AuditClient.ini

Dateibeschreibung

Eine Konfigurationsdatei ist in Abschnitte unterteilt. Jeder Abschnitt beginnt mit einer Kopfzeile, die in eckigen Klammern eingeschlossen ist. Beispiel: *[Abschnitt]*. Ein Abschnitt kann eine oder mehrere Anweisungen mit Zuordnungen von Parametern und Werten (*Parameter=Wert*) enthalten.

Die hier aufgeführten Tabellen enthalten alle Abschnitte und Parameter der Trust Authority-Konfigurationsdateien, die zum Zwecke der Systemverwaltung editiert werden können. Die Tabellen enthalten folgende Spalten:

- Parameter
- Beschreibung
- Wert gemäß Standardkonfiguration

Diese Spalte enthält den Standardwert, sofern vorhanden. Wenn ein Standardwert existiert, ist ein Parameter wahlfrei, andernfalls ist er erforderlich.

- Problemlos änderbar nach Standardkonfiguration?

  In dieser Spalte wird angegeben, ob ein Wert geändert werden kann oder nicht.

Dieses System ignoriert Leerzeichen. Einheiten müssen in der korrekten Reihenfolge eingegeben werden.

CA-Server - Konfigurationsdatei

Tabelle 14 auf Seite 79 enthält eine Beschreibung der Parameter der Konfigurationsdatei für CA-Server, jonahca.ini.

Tabelle 14. CA-Server - Konfigurationsdatei

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
[OIDs] Standardmechanismus zur eindeutigen Identifizierung von Elementen			
C=	OID für Land	2.5.4.6	Nein
O=	OID für Unternehmen	2.5.4.10	Nein
OU=	OID für Unternehmen	2.5.4.11	Nein
CN=	OID für allgemeinen Namen	2.5.4.3	Nein
L=	OID für Ort	2.5.4.7	Nein
ST=	OID für Bundesland	2.5.4.8	Nein
T=	OID für Titel	2.5.4.12	Nein
id-dsa=	OID für DSA	1.2.840.10040.4.1	Nein
id-dsa-with-sha1=	OID für DSA mit SHA-1	1.2.840.10040.4.3	Nein
rsaEncryption=	OID für RSA-Verschlüsselung	1.2.840.113549.1.1.1	Nein
sha-1WithRSAEncryption=	OID für SHA-1 mit RSA-Verschlüsselung	1.2.840.113549.1.1.5	Nein
sha1=	OID für SHA-1	1.3.14.3.2.26	Nein
hmac-sha1=	OID für SHA-1- Hash-Nachrichtenauthentifizierungscode	1.3.6.1.5.5.8.1.2	Nein
pkcs7-data=	OID für PKCS #7	1.2.840.113549.1.7.1	Nein
pkcs12-certbag=	OID für Zertifikattasche	1.2.840.113549.1.12.10.1.3	Nein
pkcs12-keybag=	OID für Schlüsseltasche	1.2.840.113549.1.12.10.1.1	Nein
X509-Certificate=	OID für X.509-Zertifikat	1.2.840.113549.1.9.22.1	Nein
PasswordBasedMAC=	OID für MAC auf Kennwortbasis	1.2.840.113533.7.66.13	Nein
MyPolicy=	Beispiel für die Eingabe einer OID für PolicyName1 im Abschnitt CertPolicy	1.34.67.7	Nein
My Lite Policy=	Beispiel für die Eingabe einer OID für PolicyName2 im Abschnitt CertPolicy	2.4.1.0	Nein
[AsymmetricKeyAlgs]			
DSA=	Definition des DSA-Schlüsselalgorithmus	id-dsa	Nein

Tabelle 14. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
RSA=	Definition des RSA-Schlüsselalgorithmus	rsaEncryption	Nein
[AsymmetricEncAlgs]			
DSA=	Definition des DSA-Verschlüsselungsalgorithmus	id-dsa	Nein
[AsymmetricSigAlgs]]			
DSAwithSHA1=	Definition des DSA mit SHA-1-Unterschriftsalgorithmus. Wird von der GUI oder dem Server zur Anzeige und zur Auswahl des Algorithmus verwendet.	id-dsa-with-sha1	Nein
RSAwithSHA1=	Definition des RSA mit SHA-1-Unterschriftsalgorithmus. Wird von der GUI oder dem Server zur Anzeige und zur Auswahl des Algorithmus verwendet.	sha-1WithRSAEncryption	Nein
[ObjectStore]			
Name=	Dateistamm (ohne Erweiterung) zur Verwendung mit CA-Datendateien	caObjectStore	Nein
Path=	Absoluter Pfad für Trust Authority CA-Dateien	Für Windows NT: c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\ Für AIX: /usr/lpp/iau/etc/TrustAuthority/	Nein
[CertPolicy] Für jeden Unterschriftsalgorithmus muß im OID-Abschnitt eine OID deklariert werden. Für jeden Regelnamen muß im OID-Abschnitt eine entsprechende OID vorhanden sein.			
SigAlg1=	Definition des ersten Unterschrifts-algorithmus. Ein entsprechender Eintrag im OID-Abschnitt ist erforderlich.	sha-1WithRSAEncryption	Nein
StartTimeSpecifiable=	Gibt an, ob der Anfordernde (Client-Entität an RA oder RA an CA) die Startzeit angeben kann.	T	Nein

Tabelle 14. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
MaxLifetime=	Die maximale Gültigkeitsdauer eines Zertifikats (in Stunden).	17544h	Ja
LifeTimeDef=	Die standardmäßige Gültigkeitsdauer eines Zertifikats (in Tagen).	180d	Nein
KeySpecifiable=	Gibt an, ob der Anfordernde (Client-Entität oder RA) den allgemeinen Schlüssel des Empfängers angeben kann.	T	Nein
KeyUsageSupported=	Gibt an, ob die Erweiterung der Schlüsselverwendung unterstützt wird.	T	Nein
KeyUsageRequired=	Gibt an, ob die Erweiterung der Schlüsselverwendung erforderlich ist.	F	Nein
PolicyCritical=	Gibt an, ob es sich um eine kritische Regel handelt.	F	Nein
PolicyRequired=	Gibt an, ob die Regel erforderlich ist.	F	Nein
PolicyName1=	Der Name der primären Regel. Hierfür muß im OID-Abschnitt eine entsprechende OID vorliegen.	MyPolicy	Nein
Policy1Org=	Der Name des Unternehmens, das diese Regel benötigt.	Ihr Unternehmen	Nein
Policy1Notice1=	Notice1 wird Policy1 zugeordnet	3	Nein
Policy1Notice2=	Notice2 wird Policy1 zugeordnet	17	Nein
UserNoticeText1=	Ein juristischer Hinweis oder eine Ablehnungserklärung, die die andere Partei lesen und bei Entscheidungen berücksichtigen muß.	Juristischer Hinweis oder Ablehnungserklärung	Nein
CPS1=	URL-Adresse, unter der die Anweisung für Policy1 verfügbar ist.	http://localhost/index.html	Nein
PolicyName2=	Name der sekundären Regel. Ist dieser Name vorhanden, muß eine entsprechende OID im OID-Abschnitt angegeben werden.	My Lite Policy	Nein

Tabelle 14. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
CPS2=	URL-Adresse, unter der die Anweisung für Policy2 verfügbar ist.	http://localhost/index.html	Nein
TimeBetweenCRLs=	Standardzeit zwischen geplanten CRL-Veröffentlichungen	1d	Ja
CRLDuration=	CRL-Gültigkeitsdauer	2d	Ja
[CrossCertPolicy]			
SigAlg1=	Definition des ersten Unterschrifts-algorithmus. Ein entsprechender Eintrag im OID-Abschnitt ist erforderlich.	sha-1WithRSAEncryption	Nein
StartTimeSpecifiable=	Gibt an, ob der Anfordernde (Client-Entität oder RA) die Startzeit angeben kann.	T	Nein
MaxLifeTime	Die maximale Gültigkeitsdauer eines Zertifikats.	17544h	Ja
LifeTimeDef	Die Standardgültigkeitsdauer eines Zertifikats.	180d	Nein
KeySpecifiable=	Gibt an, ob der Anfordernde (Client-Entität oder RA) den allgemeinen Schlüssel des Zertifikatsgegenstands angeben kann.	T	Nein
KeyUsageSupported=	Gibt an, ob die Erweiterung der Schlüsselverwendung unterstützt wird.	T	Nein
KeyUsageRequired=	Gibt an, ob die Erweiterung der Schlüsselverwendung erforderlich ist.	F	Nein
PolicyCritical=	Gibt an, ob es sich um eine kritische Regel handelt.	F	Nein
PolicyRequired=	Gibt an, ob die Regel erforderlich ist.	F	Nein
PolicyName1=	Der Name der primären Regel. Hierfür muß im OID-Abschnitt eine entsprechende OID vorliegen.	MyPolicy	Nein

Tabelle 14. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
Policy1Org=	Der Name des Unternehmens, das diese Regel benötigt.	Ihr Unternehmen	Nein
Policy1Notice1=	Notice1 wird Policy1 zugeordnet	3	Nein
Policy1Notice2=	Notice2 wird Policy1 zugeordnet	17	Nein
UserNoticeText1=	Ein juristischer Hinweis oder eine Ablehnungserklärung, die die andere Partei lesen und bei Entscheidungen berücksichtigen muß.	Juristischer Hinweis oder Ablehnungserklärung	Nein
CPS1=	URL-Adresse, unter der die Anweisung für Policy1 verfügbar ist.	http://localhost/index.html	Nein
PolicyName2=	Name der sekundären Regel.	My Lite Policy	Nein
CPS2=	URL-Adresse, unter der die Anweisung für Policy2 verfügbar ist.	http://localhost/index.html	Nein
TimeBetweenCRLs=	Standardzeit zwischen geplanten CRL-Veröffentlichungen	1d	Ja
CRLDuration=	CRL-Gültigkeitsdauer	2d	Ja
[General]			
MyName=	DN der Client-Entität.	/C=US/O=Ihr Unternehmen/OU=Trust Authority/CN=Trust Authority CA	Nein
DefaultRA=	Die Standard-RA	1	Nein
PreferredCryptoProvider=	Die GUID (Globally Unique Identifier) des Verschlüsselungsanbieters.	dda0c1e0-7b73-11d0-8e0c-0004ac602b18	Nein
CertperDP=	Zertifikate pro Verteilungspunkt	0	Ja
CRLDistName=	Name des in das Zertifikat einzutragenden Verteilungspunkts.	MyCRLDistName%d	Nein
TempPath=	Pfad zur Speicherung temporärer Dateien.	Für Windows NT: c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\ Für AIX: /usr/lpp/iau/etc/TrustAuthority/	Nein

Tabelle 14. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
PathToDLLs=	Pfad zur Speicherung von PKIX-Bibliotheken.	Für Windows NT: c:\pkix\ Für AIX: /usr/pkix/	Nein
RA1=	DN der RA für diesen CA.	/C=US/O=Ihr Unternehmen/OU=Trust Authority/CN=Trust Authority RA	Nein
[Transport]			
TCPPort=	TCP-Anschluß, der vom CA überwacht wird.	1830	Ja
TCPHost=	Host-Name der Maschine, auf der sich der CA befindet.	*Ihr Host-Name*	Nein
PollInterval=	Sendeaufrufintervall.	10s	Ja
[KeyStore]			
CurKeyStore=	Momentan verwendeter KeyStore	VSC	Nein
[VSC] Dieser Abschnitt ist erforderlich, wenn der Wert des Parameters CurKeyStore VSC lautet.			
Model=	Art des verwendeten Speichers.	PKCS11_STORAGE_MODEL	Nein
Guid=	Global Unique Identifier.	7F529C80-C942-11D1-8FB0-0004AC61389A	Nein
InitialSOpw=	Anfangskennwort für den Prüfadministrator.	SOPIN	Nein
TokenDir=	Absoluter Pfad und Dateiname für die virtuelle Smart Card.	Für Windows NT: c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\caKS.fil Für AIX: /usr/lpp/iau/etc/TrustAuthority/caKS.fil	Nein
4758GUID=	GUID für Einheit IBM 4758.	474d0880-b44c-11d1-b1cf-002035680b00	Nein
Use4758=	Gibt an, ob der CA die Einheit IBM 4758 nutzt.	false	Nein
4758ProfileUserid=	Die Benutzer-ID des 4758-Profils. Nur verfügbar bei Einstellung Use4758=true.	IBMCA001	Nein
4758ProfilePassPhrase=	Das Kennwort des 4758-Profils. Nur verfügbar bei Einstellung Use4758=true.	Secure99	Nein

Tabelle 14. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
4758Retain=	Gibt an, ob der CA die Option 4758Retain nutzt. Nur verfügbar bei Einstellung Use4758=true.	false (true nur bei Option RETAIN, die jedoch nicht empfohlen wird)	Nein
4758KeyLength=	Die Länge des 4758-Schlüssels. Mögliche Werte sind: 512,1024 und 2048. Nur verfügbar bei Einstellung Use4758=true.	512	Nein
[TrustPolicy]			
UseCRLs=	Gibt an, ob CRLs und ARLs als Teil des Prüfprozesses verwendet werden sollen.	T	Nein
AllowExpiredCRLs=	Gibt an, ob abgelaufende CRLs zulässig sind.	F	Nein
AllowFutureCRLs=	Gibt an, ob CRLs mit zukünftigen Datumsangaben zulässig sind.	F	Nein
AllowExpiredCertificates=	Gibt an, ob abgelaufene Zertifikate zulässig sind.	F	Nein
AllowFutureCertificates=	Gibt an, ob Zertifikate mit zukünftigen Datumsangaben zulässig sind.	F	Nein
AllowCRLSearchToFail=	Gibt an, ob ein Fehler vorliegt, wenn keine CRLs oder ARLs für einen Aussteller gefunden werden.	F	Nein
MaximumChainSearchDepth=	Maximale Verkettungstiefe bei rekursiven breitenorientierten Verkettungen	15	Nein
[RemoteServer]			
MaxSessions=	Optimierungsparameter.	16	Nein
EncryptionPolicy=	Gibt an, ob für die Verbindung zwischen einem Hintergrund-Server und dessen fernem Administrator eine Verschlüsselungsregel angewendet wird, wenn sich beide auf dem selben System befinden.	F	Nein

Tabelle 14. CA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
NumAdmins=	Anzahl der zertifizierten Administratoren.	0	Nein
Admin1DN=	DN von Administrator1.	Nicht verwendet	Nein
[ICL]			
IclOdbcProvider=	Art des Anbieters für ODBC.	UDB	Nein
IclProtectionPolicy	ICL-Schutzregel. Werte: Ignore ContinueWithMessage TerminateTransaction	ContinueWithMessage	Ja
IclOdbcDriverConnect=	Name der Datenbank für ICL.	DSN=ibmdb	Nein
MACLabel=	Kennsatz für MAC-Schlüssel in KeyStore.	CA_MAC_Key	Nein
[URL-Adressen]			
/C%EQ%US/O%EQ%Ihr Unternehmen/OU%EQ%Trust Authority/CN%EQ%Trust Authority RA=pkix://localhost:829	Dieser Eintrag wird bei der Konfiguration mit der URL-Adresse und dem DN für die RA gesetzt.	RA DN	Ja

RA-Server - Konfigurationsdatei

Tabelle 15 auf Seite 88 enthält Informationen zu den Parametern der RA-Server-Konfigurationsdatei jonahra.ini.

Tabelle 15. RA-Server - Konfigurationsdatei

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
[OIDs]			
C=	OID für Land	2.5.4.6	Nein
O=	OID für Unternehmen	2.5.4.10	Nein
OU=	OID für Organisationseinheit	2.5.4.11	Nein
CN=	OID für allgemeinen Namen	2.5.4.3	Nein
L=	OID für Ort	2.5.4.7	Nein
ST=	OID für Bundesland	2.5.4.8	Nein
T=	OID für Titel	2.5.4.12	Nein
id-dsa=	OID für DSA	1.2.840.10040.4.1	Nein
id-dsa-with-sha1=	OID für DSA mit SHA-1	1.2.840.10040.4.3	Nein
rsaEncryption=	OID für RSA-Verschlüsselung	1.2.840.113549.1.1.1	Nein
sha-1WithRSAEncryption=	OID für SHA-1 mit RSA-Verschlüsselung	1.2.840.113549.1.1.5	Nein
sha1=	OID für SHA-1	1.3.14.3.2.26	Nein
hmac-sha1=	OID für SHA-1- Hash-Nachrichtenauthentifizierungscode	1.3.6.1.5.5.8.1.2	Nein
pkcs7-data=	OID für PKCS #7	1.2.840.113549.1.7.1	Nein
pkcs12-certbag=	OID für PKCS #12-Zertifikatstasche	1.2.840.113549.1.12.10.1.3	Nein
pkcs12-keybag=	OID für PKCS #12-Schlüsseltasche	1.2.840.113549.1.12.10.1.1	Nein
X509-Certificate=	OID für X.509-Zertifikat	1.2.840.113549.1.9.22.1	Nein
PasswordBasedMAC=	OID für MAC auf Kennwortbasis.	1.2.840.113533.7.66.13	Nein
MyPolicy=	Beispiel für die Eingabe einer OID für PolicyName1 im Abschnitt CertPolicy	1.34.67.7	Nein
My Lite Policy=	Beispiel für die Eingabe einer OID für PolicyName2 im Abschnitt CertPolicy	2.4.1.0	Nein
[AsymmetricKeyAlgs]			

Tabelle 15. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
DSA=	Definition des DSA-Schlüsselalgorithmus	id-dsa	Nein
RSA=	Definition des RSA-Algorithmus	rsaEncryption	Nein
[AsymmetricEncAlgs]			
DSA=	Definition des DSA-Verschlüsselungsalgorithmus	id-dsa	Nein
[AsymmetricSigAlgs]]			
DSAwithSHA1=	Definition des DSA mit SHA-1-Unterschriftsalgorithmus. Wird von der GUI oder dem Server zur Anzeige und zur Auswahl des Algorithmus verwendet.	id-dsa-with-sha1	Nein
RSAwithSHA1=	Definition des RSA mit SHA-1-Unterschriftsalgorithmus. Wird von der GUI oder dem Server zur Anzeige und zur Auswahl des Algorithmus verwendet.	sha-1WithRSAEncryption	Nein
[ObjectStore]			
Name=	Dateiname ohne Erweiterung für RA-Datendateien.	raObjectStore	Nein
Path=	Absoluter Pfad für Trust Authority-RA-Datendateien.	Für Windows NT: c:\Program Files\IBM\Trust Authority\pkrf\Domains\YourDomain\etc\ Für AIX: /usr/lpp/iau/pkrf/Domains/YourDomain/etc/	Nein
[IssuerCertPolicy] Für jeden Unterschriftsalgorithmus muß im OID-Abschnitt eine OID deklariert werden. Für jeden Regelnamen muß im OID-Abschnitt eine entsprechende OID vorhanden sein.			
SigAlg1=	Definition des Unterschrifts-algorithmus. Ein entsprechender Eintrag im OID-Abschnitt ist erforderlich.	sha-1WithRSAEncryption	Nein

Tabelle 15. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
StartTimeSpecifiable=	Gibt an, ob der Anfordernde (Client-Entität an RA oder RA an CA) die Startzeit angeben kann.	T	Nein
MaxLifeTime=	Die maximale Gültigkeitsdauer eines Zertifikats.	8760h	Nein
LifeTimeDef=	Die standardmäßige Gültigkeitsdauer eines Zertifikats.	180d	Nein
KeySpecifiable=	Gibt an, ob der Anfordernde (Client-Entität oder RA) den allgemeinen Schlüssel des Empfängers angeben kann.	T	Nein
KeyUsageSupported=	Gibt an, ob die Erweiterung der Schlüsselverwendung unterstützt wird.	T	Nein
KeyUsageRequired=	Gibt an, ob die Erweiterung der Schlüsselverwendung erforderlich ist.	F	Nein
PolicyCritical=	Gibt an, ob es sich um eine kritische Regel handelt.	F	Nein
PolicyRequired=	Gibt an, ob die Regel erforderlich ist.	F	Nein
PolicyName1=	Der Name der primären Regel. Hierfür muß im OID-Abschnitt eine entsprechende OID vorliegen.	MyPolicy	Nein
Policy1Org=	Der Name des Unternehmens, das diese primäre Regel benötigt.	Ihr Unternehmen	Nein
Policy1Notice1=	Notice1 wird Policy1 zugeordnet.	3	Nein
Policy1Notice2=	Notice2 wird Policy2 zugeordnet.	17	Nein
UserNoticeText1=	Ein juristischer Hinweis oder eine Ablehnungserklärung, die die andere Partei lesen und bei Entscheidungen berücksichtigen muß.	Juristischer Hinweis oder Ablehnungserklärung	Nein

Tabelle 15. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
CPS1	URL-Adresse, unter der die Anweisung für Policy1 verfügbar ist.	http://localhost/index.html	Nein
PolicyName2=	Name der sekundären Regel. Ist dieser Name vorhanden, muß eine entsprechende OID im OID-Abschnitt angegeben werden.	My Lite Policy	Nein
CPS2=	URL-Adresse, unter der die Anweisung für Policy2 verfügbar ist.	http://localhost/index.html	Nein
EERevokeRequests=	Gibt an, ob eine Client-Entität den Widerruf eines Zertifikats anfordern kann. Lautet der Wert ANY, kann die Client-Entität den Widerruf eines von ihr angeforderten Zertifikats anfordern. Lautet der Wert NONE, kann die Client-Entität den Widerruf eines Zertifikats nicht anfordern.	Any	Nein
[IssuerCrossCertPolicy]			
SigAlg1=	Name des ersten Unterschrifts-algorithmus. Ein entsprechender Eintrag im OID-Abschnitt ist erforderlich.	sha-1WithRSAEncryption	Nein
StartTimeSpecifiable=	Gibt an, ob der Anfordernde (Client-Entität oder RA) die Startzeit angeben kann.	T	Nein
KeySpecifiable=	Gibt an, ob der Anfordernde (Client-Entität oder RA) den allgemeinen Schlüssel des Empfängers angeben kann.	T	Nein
KeyUsageSupported=	Gibt an, ob die Erweiterung der Schlüsselverwendung unterstützt wird.	T	Nein

Tabelle 15. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
KeyUsageRequired=	Gibt an, ob die Erweiterung der Schlüsselverwendung erforderlich ist.	F	Nein
PolicyCritical=	Gibt an, ob es sich um eine kritische Regel handelt.	F	Nein
PolicyRequired=	Gibt an, ob die Regel erforderlich ist.	F	Nein
PolicyName1=	Der Name der primären Regel. Hierfür muß im OID-Abschnitt eine entsprechende OID vorliegen.	MyPolicy	Nein
Policy1Org=	Der Name des Unternehmens, das diese primäre Regel benötigt.	Ihr Unternehmen	Nein
Policy1Notice1=	Notice1 wird Policy1 zugeordnet.	3	Nein
Policy1Notice2=	Notice2 wird Policy1 zugeordnet.	17	Nein
UserNoticeText1=	Ein juristischer Hinweis oder eine Ablehnungserklärung, die die andere Partei lesen und bei Entscheidungen berücksichtigen muß.	Juristischer Hinweis oder Ablehnungserklärung	Nein
CSP1	URL-Adresse, unter der die Anweisung für Policy1 verfügbar ist.	http://localhost/index.html	Nein
PolicyName2=	Name der sekundären Regel	My Lite Policy	Nein
CPS2=	URL-Adresse, unter der die Anweisung für Policy2 verfügbar ist.	http://localhost/index.html	Nein

Tabelle 15. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
EERevokeRequests=	Gibt an, ob eine Client-Entität den Widerruf eines Zertifikats anfordern kann. Lautet der Wert ANY, kann die Client-Entität den Widerruf eines beliebigen Zertifikats anfordern. Lautet der Wert SELF, kann die Client-Entität den Widerruf eines von ihr angeforderten Zertifikats anfordern. Lautet der Wert NONE, kann die Client-Entität den Widerruf eines Zertifikats nicht anfordern.	ANY	Nein
[General]			
MyName	Registrierter Name der Entität.	/C=US/O=Ihr Unternehmen/OU=Trust Authority/CN=Trust Authority RA	Nein
Issuer1	Registrierter Name des CA dieser RA.	/C=US/O=Ihr Unternehmen/OU=Trust Authority/CN=Trust Authority CA	Nein
Issuer1URL1	URL-Adresse des CA dieser RA.	pkix://servername:1830	Ja
TempPath=	Pfad zur Speicherung temporärer Dateien.	Für Windows NT: c:\Program Files\IBM\Trust Authority\pkrf\Domains\YourDomain\etc\ Für AIX: /usr/lpp/iau/pkrf/Domains\YourDomain/etc/	Nein
PathToDLLs=	Pfad zur Installation von PKIX-Bibliotheken.	Für Windows NT: c:\pkix\ Für AIX: /usr/pkix/	Nein
[Transport]			
TCPPort=	TCP-Anschluß, der von der RA überwacht wird.	829	Ja
TCPHost=	TCP/IP-Host-Name der Maschine, auf der sich die RA befindet.	Ihr Host-Name	Nein
PollInterval=	Sendeaufrufintervall.	30s	Ja

Tabelle 15. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
RetryInterval=	Die Zeit zwischen den CA-Abfragen durch die RA, sofern der vom CA an die RA übermittelte Zeitpunkt für den Sendeaufruf vor der aktuellen Uhrzeit der RA liegt.	1m	Ja
[KeyStore]			
CurKeyStore=	Momentan verwendeter KeyStore	VSC	Nein
[VSC] Dieser Abschnitt ist erforderlich, wenn der Wert des Parameters CurKeyStore VSC lautet.			
Model=	Art des verwendeten Speichers.	PKCS11_STORAGE_MODEL	Nein
GUID=	Global Unique Identifier.	7F529C80-C942-11D1-8FB0-0004AC61389A	Nein
InitialSOpw=	Anfangskennwort für den Prüfadministrator.	SOPIN	Nein
TokenDir=	Absoluter Pfad und Dateiname für die virtuelle Smart Card.	Für Windows NT: c:\Public Files\IBM\Trust Authority\pkrf\Domains\YourDomain\etc\raKS.fil Für AIX: /usr/lpp/iau/pkrf/Domains/YourDomain/etc/raKS.fil	Nein
[TrustPolicy]			
UseCRLs=	Gibt an, ob CRLs und ARLs als Teil des Prüfprozesses verwendet werden sollen.	T	Nein
AllowExpiredCRLs=	Gibt an, ob abgelaufene CRLs zulässig sind.	F	Nein
AllowFutureCRLs=	Gibt an, ob CRLs mit zukünftigen Datumsangaben zulässig sind.	F	Nein
AllowExpiredCertificates=	Gibt an, ob abgelaufene Zertifikate zulässig sind.	F	Nein
AllowFutureCertificates=	Gibt an, ob Zertifikate mit zukünftigen Datumsangaben zulässig sind.	F	Nein

Tabelle 15. RA-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Wert gemäß Standardkonfiguration	Problemlos änderbar nach Konfiguration?
ApplyNameConstraintsToEEOnly=	Gibt an, ob Namens-einschränkungen für alle oder nur für das letzte Zertifikat in der Kette angewendet werden sollen.	F	Nein
AllowCRLSearchToFail=	Gibt an, ob ein Fehler vorliegt, wenn keine CRLs oder ARLs für einen Aussteller gefunden werden.	F	Nein
MaximumChainSearchDepth=	Maximale Verkettungstiefe bei rekursiven breitenorientierten Verkettungen	15	Nein
[LDAP]			
NumServers=	Anzahl von LDAP-Servern.	1	Nein
Server1=	Host-Name und Anschluß-Nummer für den LDAP-Server.	hostname:port	Ja
AuthName1	DN des Directory-Administrators	/C=US/O=Ihr Unternehmen/OU=Trust Authority/CN=DirAdmin	Nein
AuthPwd1	Kennwort des Directory-Administrators (nur mit dem Trust Authority-Dienstprogramm 'Change Password' ändern)	Secure99	Ja
PostInterval=	Intervall, in dem geprüft wird, ob Informationen zum Senden an das Directory vorliegen.	5m	Ja
[RemoteServer]			
MaxSessions=	Optimierungsparameter.	16	Nein
EncryptionPolicy=	Gibt an, ob für die Verbindung zwischen einem Hintergrund-Server und dessen fernem Administrator eine Verschlüsselungsregel angewendet wird, wenn sich beide auf dem selben System befinden.	F	Nein
NumAdmins=	Anzahl der zertifizierten Administratoren.	0	Nein

Tabelle 15. RA-Server - Konfigurationsdatei (Forts.)

Parameter	**Beschreibung**	**Wert gemäß Standardkonfiguration**	**Problemlos änderbar nach Konfiguration?**
Admin1DN=	DN von Administrator1.	Nicht verwendet	Nein
CurrentAdminPort	Aktueller Verwaltungsanschluß	Nicht verwendet	Nein
[ICL]			
IclOdbcProvider	Art des ODBC-Anbieters.	UDB	Nein
IclOdbcDriverConnect	Name der Datenbank für ICL.	DSN=pkrfdb	Nein
[URL-Adressen]			
/C%EQ%US/O%EQ%Ihr Unternehmen/OU%EQ%Trust Authority/ CN%EQ%Trust Authority CA=pkix://localhost:1830	Dieser Eintrag wird bei der Konfiguration mit der URL-Adresse und dem DN für den CA definiert.	CA DN	Ja

Prüf-Server - Konfigurationsdatei

Die Konfigurationsdatei des Prüf-Servers, AuditServer.ini, definiert die Konfigurationsvariablen des Prüf-Servers. Diese Variablen konfigurieren die grundlegenden Funktionsmerkmale des Servers und definieren das Protokollieren von Debug- und Fehlernachrichten. Die Variablen legen außerdem fest, welche Ereignisse protokolliert werden. Die nachfolgenden Abschnitte enthalten zusätzliche Informationen zu den Einträgen in Tabelle 16 auf Seite 98.

- Generische Parameter von Servicesteuerroutinen
- Bewertungsstufen für Ereignisse
- Trace-Stufen

Generische Parameter von Servicesteuerroutinen

Folgende Parameter für Servicesteuerroutinen können für jeden Service verwendet werden:

- service.count - Die Anzahl verfügbarer Services
- service.x.name - Der Name eines Services
- service.x.classname - Der Klassenname eines Services
- service.x.dpolicy - Der Klassenname einer Übergaberegel
- service.default.count - Die Anzahl der Standardservices
- service.default.x.name - Der Name eines Standardservices

Trace-Stufen

Es existieren folgende Trace-Stufen:

- All - Protokollierung von Fehler-, Warnungs-, Informations- und Trace-Nachrichten
- Error - Protokollierung von Fehlernachrichten
- Warning - Protokollierung von Fehlernachrichten und Warnungen
- Eventinfo - Protokollierung von Fehler- und Trace-Nachrichten
- None - Keine Protokollierung von Nachrichten

Tabelle 16. Prüf-Server - Konfigurationsdatei

Parameter	Beschreibung	Standardwert	Problemlos änderbar nach Konfiguration?
Server-Anschluß			
acceptor.classname=	Der Name der Acceptor-Klasse.	com.ibm.irg.sysmgmt.daemon.acceptors.SMSocketAcceptor	Nein
acceptor.arg=	Der Anschluß, der vom Prüf-Server überwacht wird.	7222	Ja
acceptor.init.retries=	Anzahl der Bindungsversuche am Server-Socket	3	Ja
acceptor.init.delay=	Die Anzahl an Sekunden, die zwischen zwei Bindungsversuchen gewartet werden soll. (Das Programm geht von Sekunden aus.)	3	Ja
Servicesteuerroutine			
service.count=	Die Anzahl verfügbarer Services	2	Nein
Protokoll-Service			
service.1.name=	Der Name des Protokollservices	log	Nein
service.1.classname=	Der Klassenname des Protokollservices	com.ibm.irg.sysmgmt.daemon.services.log.SMLogService	Nein
service.1.dpolicy=	Der Klassenname der Übergaberegel des Protokollservice.	com.ibm.irg.sysmgmt.daemon.services.log.SMLogDeliveryPolicy	Nein
Prüf-Service			
service.2.name=	Der Name des Prüfservices	audit	Nein
service.2.classname=	Der Klassenname des Prüfservices	com.ibm.irg.sysmgmt.daemon.services.audit.SMAuditService	Nein
service.2.dpolicy=	Der Klassenname der Übergaberegel des Prüfservices	com.ibm.irg.sysmgmt.daemon.services.audit.SMAuditDeliveryPolicy	Nein
Standardservices			
service.default.count=	Die Anzahl verfügbarer Standard-services	2	Nein
service.default.1.name=	Der Name des Standardservices	log	Nein
service.default.2.name=	Der Name des Standardservices	audit	Nein
Ereigniskonfiguration			
irgsmd.event.config=	Die Ereigniskonfigurationsdatei	smevents.conf	Nein

Tabelle 16. Prüf-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Standardwert	Problemlos änderbar nach Konfiguration?
Ereignisprotokoll			
event.log.filename=	Die Datei zur Aufzeichnung von Ereignissen.	Für Windows NT: c:\\Program Files\\IBM\\Trust Authority\\logs\\smevents.log Für AIX: /usr/lpp/iau/logs/smevents.log	Ja
event.log.append=	Markierung, die angibt, ob Daten an das Ereignisprotokoll angefügt werden oder ob dieses überschrieben wird.	true	Ja
Prüfung			
audit.ksfile=	Die KeyStore-Prüfdatei. Diese Datei wird zum Speichern der Prüf-Chiffrierschlüssel verwendet.		Nein
audit.catalog	Der Dateiname der NLS-Katalogdatei.	Für Windows NT: c:\\Program Files\\IBM\\Trust Authority\\catalog\\IRGVDS.DLL Für AIX: /usr/lpp/iau/catalog/IRGVDS.cat	Nein
audit.db.instance=	Der Name des DB2-Prüfexemplars.		Nein
audit.db.name=	Der Name der Prüfdatenbank.		Nein
audit.db.connection=	Der Algorithmus zur Verwaltung der Datenbankverbindung.	single	Nein
audit.log.connect.retries=	Die Anzahl der zulässigen Versuche zur Herstellung einer Verbindung zur Datenbank/Protokolldatei.	3	Ja
audit.log.update.retries=	Die Anzahl der zulässigen Versuche zur Aktualisierung des Prüfprotokolls.	3	Ja
audit.log.timeout	Der zulässige Zeitlimitüberschreitungswert zur Aktualisierung des Prüfprotokolls.	60s	Ja
audit.log.integrity=	Aktivieren oder Inaktivieren der Integritätsprüfung.	true	Nein
Trace			

Tabelle 16. Prüf-Server - Konfigurationsdatei (Forts.)

Parameter	Beschreibung	Standardwert	Problemlos änderbar nach Konfiguration?
trace.enable=	Eine Markierung zur Aktivierung/Inaktivierung der Trace-Funktion.	false	Ja
trace.level.name=	Der Name für eine Trace-Stufe	all	Ja
trace.event.enable=	Aktivieren/Inaktivieren der Trace-Funktion für Ereignisse	false	Nein
trace.log.filename=	Der Name der Trace-Protokolldatei.	Für Windows NT: c:\\Program Files\\IBM\\Trust Authority\\logs\\iausmd.log Für AIX: /usr/lpp/iau/logs/iausmd.log	Ja
trace.log.append=	Markierung, die angibt, ob Daten an die vorhandene Trace-Datei angefügt werden oder ob diese überschrieben wird	true	Ja
Fehler			
error.log.filename=	Der Name der Fehlerdatei.	Für Windows NT: c:\\Program Files\\IBM\\Trust Authority\\logs\\iausmd.err Für AIX: /usr/lpp/iau/logs/iausmd.err	Ja

Prüf-Client-Konfigurationsdatei AuditClient.ini

Die Konfigurationsdatei des Prüf-Clients, AuditClient.ini, definiert die Konfigurationsvariablen des Prüf-Clients.

Tabelle 17. Prüf-Client - Konfigurationsdatei

Parameter	**Beschreibung**	**Standardwert**	**Problemlos änderbar nach Konfiguration?**
Verbindungseinstellungen			
[CONNECTION]			
EnableAudit=	Aktivieren/Inaktivieren von Prüfereignissen	true	Nein
HostName=	Prüf-Server-Host	*Ihr Host-Name*	Nein
Port=	Anschluß des Prüf-Servers. Muß mit dem in der Datei 'AuditServer.ini' angegebenen Anschluß übereinstimmen.	59998	Ja
AuthType=	Authentifizierungsmechanismus. Dieser Parameter wird in diesem Release von Trust Authority nicht unterstützt.	Keiner	Nein
UseSSL=	Soll SSL für die Client/Server-Sitzung verwendet werden? Für zukünftige Sitzungen. Dieser Parameter wird in diesem Release von Trust Authority nicht unterstützt.	Nein	Nein
SSLKeyDB=	SSL-Schlüsseldatenbank. Dieser Parameter wird in diesem Release von Trust Authority nicht unterstützt.	Für AIX: /usr/lpp/iau/audit/client/ssl.kdb Für Windows NT: c:\Program Files\IBM\Trust Authority\audit\client\ssl.kdb	Nein
SSLv2Token=	SSL-Schlüsseldatenbank-Token. Dieser Parameter wird in diesem Release von Trust Authority nicht unterstützt.	Token	Nein
Retries=	Anzahl von Sendeversuchen für ein Ereignis	4	Ja
Timer	Die Zeit in Millisekunden, die zwischen den Wiederholungsversuchen für das Herstellen einer Verbindung zum Server gewartet werden soll.	1000	Ja
Abschnitte für Komponentenmasken			
[CA]			
ExcludedEvents=	CA-Ereignisse, die nicht gesendet werden		Ja
[RA]			
ExcludedEvents=	RA-Ereignisse, die nicht gesendet werden	ReceiptOfCertRequest	Ja

Befehlszeilendienstprogramme

Dieser Abschnitt enthält Beschreibungen der Syntax und der Parameter für folgende Befehlszeilendienstprogramme:

- Dienstprogramm CA Certification
- Dienstprogramm Add RA User
- Dienstprogramm Enable RA Encryption
- Dienstprogramm Audit Archive and Sign
- Dienstprogramm Audit Integrity Check

Dienstprogramm CA Certification

Das Dienstprogramm CA Certification ermöglicht Ihnen, von einem anderen CA Zertifizierungen im Namen des Trust Authority-CA anzufordern. Hierzu stehen Ihnen das Modell zur gegenseitigen Zertifizierung und das hierarchische Sicherungsmodell zur Verfügung.

Anmerkung: Wenn Sie planen, als Teil Ihrer allgemeinen Hierarchielösung die hierarchischen CA-Zertifikate in Netscape Communicator herunterzuladen, sollten Sie die Markierung ″-m ..″ mit dem Dienstprogramm CA Certification verwenden, um die Erweiterung 'Name Constraints' aus dem resultierenden CA-Zertifikat auszuschließen. Mit Ausnahme von ″-m ..″ sollten Sie keine anderen der Name Constraints-Befehlszeilenoptionen (also nicht -i/I, -d/D, -u/U, -n/N oder -m/M) mit dem Dienstprogramm CA Certification verwenden. Beispiel: Ein Exemplar eines solchen Befehls könnte folgendermaßen aussehen:

```
CaCertRq -m .. -h -r "c:\Program Files\IBM\Trust Authority\ccprereg.reg"
   -P 1835 -W Secure99
```

Syntax

Die Syntax für dieses Dienstprogramm lautet wie folgt:

```
CaCertRq
    [-i ipAddressMask [-I ipAddressMask]]
    [-d dns [-D dns]]
    [-m emailAddress [-M emailAddress]]
    [-u uri [-U uri]]
    [-n directoryName [-N directoryName]]
    [-p inhibitPolMap]
    [-h [-m ..]]
    [-C filename | -B filename]
    [-S filenames]
    -r preregistrationpath
    -P 1835
    -W password
```

Parameter

[-i *ipAddressMask* **[-I** *ipAddressMask***]]**

Die IP-Adreßmaske (IP = Internet Protocol) im CDIF-Format. Der kleingeschriebene Parameter (-i) fügt die angegebene IP-Adreßmaske der Liste zulässiger Unterverzeichnisstrukturen hinzu. Der großgeschriebene Parameter (-I) entspricht dem kleingeschriebenen Parameter. Die angegebene IP-Adreßmaske wird jedoch der Liste unzulässiger Unterverzeichnisstrukturen hinzugefügt.

Die Maske des Unternehmens X lautet beispielsweise 9.0.0.0/255.0.0.0 und die der Abteilung Y dieses Unternehmens lautet 9.210.134.0/255.255.254.0.

[-d *dns* **[-D** *dns***]]**
Die Adresse des Domain Name Server (DNS). Der kleingeschriebene Parameter (-d) fügt die angegebene DNS-Adresse der Liste zulässiger Unterverzeichnisstrukturen hinzu. Der großgeschriebene Parameter (-D) entspricht dem kleingeschriebenen Parameter. Die angegebene DNS-Adresse wird jedoch der Liste unzulässiger Unterverzeichnisstrukturen hinzugefügt.

Beginnt die Adresse mit einem Punkt, werden alle Hosts einbezogen, die mit dieser Unterzeichenfolge (einschließlich ".") enden. Ist dies nicht der Fall, wird nur der Host einbezogen, der der Zeichenfolge entspricht.

Der Einschränkung ".orga.com" entsprechen beispielsweise die Hosts us.orga-.com, vneto.orga.com und w3.software.orga.com, jedoch nicht orga.com selbst oder kidorga.com. Der Einschränkung orga.com entspricht der Host orga.com, jedoch nicht us.orga.com oder die anderen. Daraus folgt, daß eine zulässige Unterverzeichnisstruktur ohne führenden Punkt nur einen möglichen Knoten angibt.

[-m *emailAddress* **[-M** *emailAddress***]]**
Die E-Mail-Adressen. Der kleingeschriebene Parameter (-m) fügt die angegebene E-Mail-Adresse der Liste zulässiger Unterverzeichnisstrukturen hinzu. Der großgeschriebene Parameter (-M) entspricht dem kleingeschriebenen Parameter. Die angegebene E-Mail-Adresse wird jedoch der Liste unzulässiger Unterverzeichnisstrukturen hinzugefügt.

Eine E-Mail-Adresse kann im Standardformat (ohne Platzhalter) oder als DNS-Adresse angegeben werden. Die Regeln für eine DNS-Adresse entsprechen den Regeln für die Option -d. Daraus folgt, daß eine zulässige Unterverzeichnisstrukturen mit einer Standard-E-Mail-Adresse nur einen möglichen Benutzer angibt.

[-u *uri* **[-U** *uri***]]**
Die URI. Der kleingeschriebene Parameter (-u) fügt die angegebene URI der Liste zulässiger Unterverzeichnisstrukturen hinzu. Der großgeschriebene Parameter (-U) entspricht dem kleingeschriebenen Parameter. Die angegebene URI wird jedoch der Liste unzulässiger Unterverzeichnisstrukturen hinzugefügt.

Der Knotenabschnitt der URI (Uniform Resource Identifier) unterliegt den gleichen Regeln wie die Option -d, sofern er keine IP-Adresse enthält. In diesem Fall wird er als exakte Übereinstimmung behandelt.

[-n *directoryName* **[-N** *directoryName***]]**
Der Directory-Name. Der kleingeschriebene Parameter (-n) fügt das angegebene Directory der Liste zulässiger Unterverzeichnisstrukturen hinzu. Der großgeschriebene Parameter (-N) entspricht dem kleingeschriebenen Parameter. Das angegebene Directory wird jedoch der Liste unzulässiger Unterverzeichnisstrukturen hinzugefügt.

Diese Namen müssen im LDAP-Standardformat angegeben werden. Namen, die dem Ende der angegebenen RDNs (Relative Distinguished Names) entsprechen, gelten als exakte Übereinstimmung, auch wenn andere RDNs vorhanden sind.

Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (" ") setzen.

[-h]
Gibt an, daß die Zertifikatsanforderung das hierarchische Sicherungsmodell verwendet.

[-m ..]
Gibt an, daß die Erweiterung für Namenseinschränkungen (Name Constraints) aus dem Zertifikat ausgeschlossen wird.

[-C *filename***]**
Gibt den Namen der Datei an, in die die binärcodierte Anforderung PKCS #10 geschrieben wird. Die Parameter -C und -B schließen sich gegenseitig aus.

[-B *filename***]**
Gibt den Namen der Datei an, in die die Base 64-binärcodierte Anforderung PKCS #10 geschrieben wird. Die Parameter -C und -B schließen sich gegenseitig aus.

[-S *filename***]**
Gibt den Namen der Datei an, die die Antwort für PKCS#7 enthält.

-r *preregistrationpath*
Der Pfadname der vom ausstellenden System erzeugten Vorabregistrierungsdatei.

-P 1835
Die administrative Anschluß-Nummer des CA (1835).

-p *inhibitPolMap*
Der Wert des Erweiterungsfelds inhibitPolicyMapping.

Ist diese Option nicht vorhanden, lautet der Standardwert 1.

-W *password*
Das bei der Erzeugung der Vorabregistrierungsdatei eingegebene Kennwort.

Dienstprogramm Add RA User

Mit dem Dienstprogramm Add RA User können Sie der angegebenen Trust Authority-Registrierungsdomäne einen administrativen RA-Benutzer (oder einen Registrator) hinzufügen.

Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (″ ″) setzen.

Syntax

```
add_rauser domain_configuration_file domain_name ID
[access_profile]
```

Parameter

domain_configuration_file
Der absolute Pfad zur Domänenkonfigurationsdatei (domain.cfg). Diese Datei enthält einen Abschnitt für jede im System konfigurierte Registrierungsdomäne. Auf diese Weise können Sie das virtuelle Stammverzeichnis der angegebenen Registrierungsdomäne lokalisieren.

domain_name
Der Name der Registrierungsdomäne, die der hinzugefügte Registrator verwalten soll.

ID Entweder die vom Browser zum Zeitpunkt der Zertifikatsanforderung an den

Benutzer zurückgegebene ID oder die Identitätsnachweis-UUID, die Sie erhalten, wenn Sie mit Hilfe von RA Desktop den Zertifikatseintrag des Benutzers anzeigen.

Wenn Sie den Parameter für die ID angeben, geht das Programm zunächst davon aus, daß es sich bei der ID um eine Anforderungs-ID handelt. Es verwendet anschließend diesen Wert, um die Identitätsnachweis-UUID festzustellen (beispielsweise `sp0ApHvpzvCicr1Ts8ssKw==`). Das Zertifikat muß also bereits zuvor an den Benutzer ausgestellt worden sein, der die Berechtigung als Registrator anfordert.

Kann kein übereinstimmender Eintrag in der Registrierungsdatenbank gefunden werden, geht das Programm davon aus, daß es sich bei der ID um eine Identitätsnachweis-UUID handelt. Es versucht, einen entsprechenden Anforderungseintrag zu finden. Kann keine Übereinstimmung gefunden werden, gibt das Programm eine Warnung aus und versucht, einen Eintrag zur Tabelle der Registratoren (rausers) in der Datenbank hinzuzufügen.

access_profile
Ein wahlfreier Parameter, der das Zugriffsprofil angibt, das dem Registrator zugeordnet ist, den Sie dem System hinzufügen. Wenn Sie keinen Wert angeben, verwendet das Programm den Standardwert RAUser.

Bei diesem Parameter muß es sich um ein gültiges Profil handeln, das in einer der Trust Authority-Konfigurationsdateien für die Registrierungsverwaltung angegeben wurde. Das Profil enthält die Anforderungsarten, Aktionen etc., die die zugeordneten Registratoren ausführen können.

Dienstprogramm Enable RA Database Encryption

Standardmäßig werden Informationen in der Datenbank der Registrierungsfunktion nicht verschlüsselt. Nach der Konfiguration können Sie die Datenbankverschlüsselung durch Ausführen des Programms Enable RA Database Encryption (iauEnableRADBSec) aktivieren.

Syntax

`iauEnableRADBSec -d` *`domain_name`* `-r` *`install_directory`* `[i]`

Parameter

-d *domain_name*
Der Name Ihrer Registrierungsdomäne. Dieser Wert muß mit dem Wert übereinstimmen, der im Setup Wizard für den Registrierungsdomänennamen angegeben wurde.

-r *install_directory*
Der vollständige Pfad, unter dem Trust Authority installiert ist.

-i *install_directory*
Ein wahlfreier Parameter, über den das System angewiesen wird, Debug-Nachrichten (derzeit nur in Englisch) anzuzeigen.

Dienstprogramm Audit Archive and Sign

Mit dem Dienstprogramm Audit Archive and Sign können Sie Prüfprotokolldateien archivieren und unterzeichnen.

Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (″ ″) setzen.

Syntax

```
AuditArchiveAndSign [-c ConfigFile-Pfad] [-n] ArchiveFileName
```

Parameter

-c *ConfigFilePath*
Der absolute Pfad der Konfigurationsdatei des Prüf-Servers.

- Der Standardpfad für AIX lautet: /usr/lpp/iau/etc/TrustAuthority/AuditServer.ini
- Der Standardpfad für Windows NT lautet: c:\Program Files\IBM\Trust Athority\etc\TrustAuthority\AuditServer.ini

Anmerkung: Dieser Parameter ist wahlfrei. Wenn Sie keinen Wert angeben, wird die Standardkonfigurationsdatei des Prüf-Servers angegeben.

-n Gibt an, daß Protokolleinträge nicht aus der Datenbank gelöscht werden sollen.

ArchiveFileName
Das Namenspräfix der Datei, in die die Prüfprotokolle geschrieben werden. Das Dienstprogramm fügt den Archiv- und Unterschriftsdateien die Endungen .ixf beziehungsweise .sig hinzu.

Dienstprogramm Audit Integrity Check

Das Dienstprogramm Audit Integrity Check prüft die Integrität von Protokolleinträgen sowohl in Archiven als auch in der Datenbank des Prüf-Servers. Dieses Tool kann nur dann eingesetzt werden, wenn Integritätsprüfungen auf Ihrem System aktiviert wurden. Die Syntaxformate für diesen Befehl lauten wie folgt:

- Format 1

  Dieses Format prüft die Integrität der Datenbank des Prüf-Servers und fordert Sie zur Eingabe des Prüfadministratorkennworts auf.
- Format 2

  Diese Format prüft die Integrität einer oder mehrerer Archivdateien des Prüf-Servers und fordert Sie zur Eingabe des Prüfadministratorkennworts auf.
- Format 3

  Dieses Format prüft die Integrität aller Archivdateien im angegebenen Verzeichnis und fordert Sie zur Eingabe des Prüfadministratorkennworts auf.

Anmerkung: Wenn Sie als Parameter eines Befehls einen Verzeichnispfad angeben, der eingebettete Leerzeichen enthält, müssen Sie den Pfad in doppelte Anführungszeichen (″ ″) setzen.

Syntax

Format 1:

```
AuditIntegrityCheck [-c ConfigFilePath] -d
```

Format 2:

```
AuditIntegrityCheck [-c ConfigFilePath] -a ArchiveFileName1 ArchiveFileName2
ArchiveFileName3
```

Format 3:

```
AuditIntegrityCheck [-c ConfigFilePath] -A ArchiveFileDirectory
```

Parameter

-c *ConfigFilePath*

Der absolute Pfad der Konfigurationsdatei des Prüf-Servers.

- Der Standardpfad für AIX lautet: /usr/lpp/iau/etc/TrustAuthority/AuditServer.ini
- Der Standardpfad für Windows NT lautet: c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\AuditServer.ini

Anmerkung: Dieser Parameter ist wahlfrei. Wenn Sie keinen Wert angeben, wird die Standardkonfigurationsdatei des Prüf-Servers angegeben.

-a *ArchiveFileName1 ArchiveFileName2 ArchiveFileName3*

Das Pfadnamenpräfix der Archivdateien, deren Integrität geprüft werden soll. Das Präfix steht für eine Gruppe von Dateien, die dem Archiv zugeordnet sind.

Der Befehl -a /local/archive/archive1-1067 verarbeitet beispielsweise mehrere Dateien mit dem Pfadnamenpräfix /local/archive/archive1-1067 wie folgt:

```
/local/archive/archive1-1067_audit_log.ixf
/local/archive/archive1-1067_audit_log.sig
```

-A *ArchiveFileDirectory*

Der Pfadname des Verzeichnisses, das die Archivdateien enthält, deren Integrität geprüft werden soll. Alle Dateien mit den Endungen _audit_log.ixf und _audit_log.sig werden geprüft.

Felder für Prüfereignisse

Der Abschnitt Tabelle 18 erläutert die Informationen, die in Trust Authority-Prüfereignissen enthalten sind.

Tabelle 18. Felder für Prüfereignisse

Feldname	Beschreibung
Ereignisname	Die Ereigniskennung, die von einem Prüf-Client als Token angegeben wird.
Betroffene Entität	Die Entität, die von der Aktion betroffen ist, für die ein Prüfereignis gesendet wird. Diese Information wird von einem Prüf-Client angegeben.
Art der betroffenen Entität	Die Art der betroffenen Entität. Diese Information wird von einem Prüf-Client angegeben.
Berechtigte Entität	Diese Entität hat die Operation berechtigt. Diese Information wird von einem Prüf-Client angegeben.
Aufgabe der berechtigten Entität	Der Aufgabenbereich der berechtigten Entität.
Speichermedium	Sofern verfügbar, das für diese Operation angegebene Speichermedium. Diese Information wird von einem Prüf-Client angegeben.
Bewertungsstufe	Die Bewertung des Ereignisses: entweder 'Information' oder 'Alert'.
Typ der berichtenden Komponente	Der Typ der Trust Authority-Komponente, die das Ereignis meldet.
Client-Quelle	Identifizierungsinformationen für die Trust Authority-Komponente, die das Ereignis sendet.
Client-Zeitmarke	Die Uhrzeit, an der das Prüfereignis von einer Trust Authority-Komponente gesendet wurde.
Zeitmarke	Die Uhrzeit, an der das Prüfereignis in die Datenbank oder in eine Datei geschrieben wurde.
Zusatzinformationen	Zusätzliche Informationen, die für die Operation relevant sind. Diese Informationen werden von einem Prüf-Client angegeben.

Prüfereignisse

Tabelle 19 erläutert die Trust Authority-Prüfereignisse und gibt an, ob ein Ereignis verbindlich oder wahlfrei ist.

Tabelle 19. Prüfereignisse

Ereignis	Beschreibung	Verbindlich oder wahlfrei
Schlüsselverwaltung		
KeyGeneration	Gibt an, daß ein Chiffrierschlüssel generiert wurde.	verbindlich
KeyImport	Gibt an, daß ein Chiffrierschlüssel in Trust Authority importiert wurde.	wahlfrei
KeyExport	Gibt an, daß ein Chiffrierschlüssel aus Trust Authority exportiert wurde.	wahlfrei
KeyStorage	Gibt an, daß ein Chiffrierschlüssel gespeichert wurde.	wahlfrei
KeyRollover	Gibt an, daß ein Chiffrierschlüssel durch einen neuen Schlüssel ersetzt wurde. Dieser Schlüssel wird für den gleichen Zweck eingesetzt wie der alte Schlüssel.	wahlfrei
KeyCompromise	Gibt an, daß ein Chiffrierschlüssel nicht mehr sicher ist.	verbindlich
CAKeyDistribution	Gibt an, daß der öffentliche Schlüssel des CA in das Directory geschrieben wurde.	verbindlich
Zertifikatsverwaltung		
CertGeneration	Gibt an, daß ein Zertifikat generiert wurde.	verbindlich
CertRevocation	Gibt an, daß ein Zertifikat widerrufen wurde.	verbindlich
CertRenewal	Gibt an, daß ein Zertifikat erneuert wurde.	verbindlich
CertSuspension	Gibt an, daß ein Zertifikat temporär ausgesetzt wurde.	verbindlich
CertResumption	Gibt an, daß ein zuvor ausgesetztes Zertifikat aktiviert wurde.	verbindlich
CRLQuery	Gibt an, daß die Zertifikatswiderrufsliste (CRL) gelesen wurde.	wahlfrei
CRLUpdate	Gibt an, daß die Zertifikatswiderrufsliste (CRL) aktualisiert wurde.	verbindlich
SubmitCertRequest	Gibt an, daß eine Zertifikatsanforderung übergeben wurde.	wahlfrei
Enrollment	Gibt an, daß eine RA eine Registrierung bei einem CA angefordert hat.	verbindlich
Unenrollment	Gibt an, daß eine RA das Aufheben einer Registrierung bei einem CA angefordert hat.	verbindlich
CertDeletion	Gibt an, daß der CA ein Zertifikat aus der Zertifikatsdatenbank gelöscht hat.	wahlfrei
Sicherheitsrelevant		
SuccessfulAuthWithPassword	Gibt an, daß ein Authentifizierungsversuch mit Hilfe eines Kennworts erfolgreich war.	verbindlich

Tabelle 19. Prüfereignisse (Forts.)

Ereignis	Beschreibung	Verbindlich oder wahlfrei
UnsuccessAuthWithPassword	Gibt an, daß ein Authentifizierungsversuch mit Hilfe eines Kennworts fehlgeschlagen ist.	verbindlich
SuccessfulAuthWithCert	Gibt an, daß ein Authentifizierungsversuch mit Hilfe eines Zertifikats erfolgreich war.	verbindlich
UnsuccessfulAuthWithCert	Gibt an, daß ein Authentifizierungsversuch mit Hilfe eines Zertifikats fehlgeschlagen ist.	verbindlich
SuccessfulCertValidation	Gibt an, daß die gesamte Zertifizierungskette bis hin zum Zertifikat des Stamm-CA geprüft wurde.	verbindlich
UnsuccessfulCertValidation	Gibt an, daß die gesamte Zertifizierungskette bis hin zum Zertifikat des Stamm-CA nicht bestätigt wurde.	verbindlich
PasswordChange	Gibt an, daß ein Kennwort erfolgreich geändert wurde.	verbindlich
ACLUpdate	Gibt an, daß ein Benutzer oder eine Entität der Zugriffssteuerungsliste (ACL) hinzugefügt oder aus der Liste gelöscht wurde.	verbindlich
SuccessfulIntegrityCheck	Gibt an, daß ein Versuch, die Integrität eines durch eine Transaktion mit einer Nicht-Trust Authority-Komponente entstandenen Protokolleintrag zu testen, erfolgreich war.	verbindlich
UnsuccessfulIntegrityCheck	Gibt an, daß ein Versuch, die Integrität eines durch eine Transaktion mit einer Nicht-Trust Authority-Komponente entstandenen Protokolleintrags zu testen, fehlgeschlagen ist.	verbindlich
SuccessfulAcquirePrivilege	Gibt an, daß die Anforderung eines bestimmten Zugriffs auf einen Trust Authority-KeyStore erfolgreich war.	verbindlich
UnsuccessfulAcquirePrivilege	Gibt an, daß die Anforderung eines bestimmten Zugriffs auf einen Trust Authority-KeyStore fehlgeschlagen ist.	verbindlich
Aktionen des Sicherheitsbeauftragten		
SOAdd	Gibt an, daß dem System ein Prüfadministrator hinzugefügt wurde.	verbindlich
SODelete	Gibt an, daß ein Prüfadministrator vom System entfernt wurde.	verbindlich
AudEventMaskChange	Gibt an, daß die Maske geändert wurde, die die Gruppe von Prüfereignissen definiert, die ein Client an den Server senden kann.	verbindlich
CACrossCertRequest	Gibt an, daß ein Zertifikat eines gegenseitig zertifizierten CA angefordert wurde.	verbindlich
CAHierarchicalCertReq	Gibt an, daß ein Zertifikat eines hierarchisch zertifizierten CA angefordert wurde.	verbindlich

Tabelle 19. Prüfereignisse (Forts.)

Ereignis	Beschreibung	Verbindlich oder wahlfrei
SubmitRevocationRequest	Gibt an, daß ein Registrator (RA-Administrator) eine Widerrufsanforderung übergeben hat.	wahlfrei
RequestSetRenewable	Gibt an, daß ein Registrator angefordert hat, ein Zertifikat mit dem Status 'erneuerbar' zu definieren.	verbindlich
RequestSetNonRenewable	Gibt an, daß ein Registrator angefordert hat, ein Zertifikat mit dem Status 'nicht erneuerbar' zu definieren.	verbindlich
RequestPend	Gibt an, daß ein Registrator angefordert hat, eine Identitätsnachweisanforderung in den Wartestatus zu setzen.	verbindlich
RA-Ereignisse		
ReceiptOfCertRequest	Gibt an, daß eine Zertifikatsanforderung von einer RA empfangen wurde.	wahlfrei
ReceiptOfRevocationRequest	Gibt an, daß eine Widerrufsanforderung für ein Zertifikat von einer RA empfangen wurde.	wahlfrei
ReceiptOfRenewalRequest	Gibt an, daß eine Erneuerungsanforderung für ein Zertifikat von einer RA empfangen wurde.	wahlfrei
RequestApproval	Gibt an, daß eine RA eine Zertifikatsanforderung bestätigt hat.	verbindlich
RequestRejection	Gibt an, daß eine RA eine Zertifikatsanforderung zurückgewiesen hat.	verbindlich
RequestCompletion	Gibt an, daß eine Zertifikatsanforderung abgeschlossen wurde.	wahlfrei
Preregistration	Gibt an, daß ein Registrator eine Anforderung zur Vorabregistrierung erhalten hat.	verbindlich

Daten der Prüfdatenbank

Die Trust Authority-Prüfdatenbank verwendet ein Schema, das auf den Empfehlungen im Standard 'Public Key Cryptography for the Financial Services Industry' (X9.57) basiert. In diesem Abschnitt werden folgende Datenbanktabellen beschrieben.

Anmerkung: In diesem Abschnitt entsprechen die Feldnamen der Prüfsätze den Spaltennamen in den Datenbanktabellen.

- Schlüssel

  Dies ist eine Steuertabelle für private/geheime Schlüssel, die zum Unterzeichnen, Verschlüsseln und Erzeugen von Nachrichtenauthentifizierungscodes (MAC) verwendet werden.
- Ereignisbewertung (event_severities)

  Diese Tabelle beschreibt die Bewertung von Ereignissen.
- Ereignissteuerung (event_ctl)

  Diese Tabelle beschreibt alle prüfbaren Ereignisse.
- Quellen

  Diese Tabelle enthält eine Liste aller Ereignisquellen.
- Berechtigte Entitäten (auth_entities)

  Diese Tabelle enthält eine Liste aller berechtigten Entitäten.
- Betroffene Entitäten (afctd_entity_types)

  Diese Tabelle enthält eine Liste aller betroffenen Aufgabenbereiche.
- Berechtigte Aufgabenbereiche (auth_roles)

  Diese Tabelle enthält eine Liste aller Aufgabenbereiche für berechtigte Entitäten.
- Komponentenarten (component_types)

  Diese Tabelle enthält eine Liste aller Komponentenarten.
- Prüfprotokoll (audit_log)

  Dies ist die Haupttabelle für Einträge im Prüfprotokoll.
- Systemereignis

  Diese Tabelle enthält Informationen, die für das gesamte Prüfsystem gelten. Die Tabelle hat nur eine Zeile.

Schlüsseltabelle

Die Schlüsseltabelle enthält Informationen zu allen vom Prüfsystem verwendeten Chiffrierschlüsseln.

Tabelle 20. Felder der Schlüsseltabelle

Feld	Beschreibung	Datentyp
key_id	Die eindeutige interne Schlüsselkennung.	smallint
alg_oid	Der dem Schlüssel zugeordnete Algorithmus.	varchar
label	Der KeyStore-Kennsatz oder ein Token zur Lokalisierung des realen Schlüssels.	varchar
integrity	Dieses Feld dient der Aufrechterhaltung der Integrität des Datensatzes.	varchar für Bitdaten

Tabelle für Ereignisbewertung

Diese Tabelle enthält Informationen zur Bewertung von Ereignissen. Diese Tabelle ist schreibgeschützt und wird bei Installation und Konfiguration geladen.

Tabelle 21. Felder in der Tabelle für die Ereignisbewertung

Feld	Beschreibung	Datentyp
severity_id	Die eindeutige interne Kennung der Ereignisbewertung.	smallint
severity_desc	Die NLS-Zeichenfolge (NLS = National Language Support) für die Bewertung.	varchar

Tabelle zur Ereignissteuerung

Diese Tabelle enthält Informationen zu allen Ereignissen, die ein Prüf-Client an den Prüf-Server weiterleiten kann. Diese Tabelle ist schreibgeschützt und wird bei Installation und Konfiguration geladen.

Tabelle 22. Felder in der Tabelle für die Ereignissteuerung

Feld	Beschreibung	Datentyp
event_id	Die eindeutige Ereigniskennung.	smallint
event_desc	Eine sichtbare Beschreibung des Ereignisses. Dieses Feld kann zur Anzeige von Informationen verwendet werden.	varchar
event_key	Eine kurze eindeutige Zeichenfolge, die das Ereignis kennzeichnet und beschreibt. Dieses Feld wird von den Java-Ressourcenpaketen verwendet.	varchar

Tabelle 22. Felder in der Tabelle für die Ereignissteuerung (Forts.)

Feld	Beschreibung	Datentyp
event_severity_id	Die Bewertungs-ID des Ereignisses. Dies ist der fremde Schlüssel, der auf die Tabelle event_severities verweist.	smallint

Quellentabelle

Diese Tabelle enthält eine Liste aller Prüf-Clients. Ein Prüf-Client ist eine Trust Authority-Komponente, die Prüfereignisse erzeugt.

Tabelle 23. Felder in der Quellentabelle

Feld	Beschreibung	Datentyp
source_id	Die eindeutige Kennung des Prüf-Clients.	smallint
Quelle	Die Kennung des Prüf-Clients, die zur Anzeige genutzt werden kann. In der Regel handelt es sich hierbei um den DN des Prüf-Clients.	varchar
Integrität	Dieses Feld dient der Aufrechterhaltung Integrität des Eintrags.	varchar für Bitdaten

Tabelle der berechtigten Entitäten

Diese Tabelle enthält eine Liste aller berechtigten Entitäten. Eine berechtigte Entität berechtigt die Operation, für die ein Prüfereignis erzeugt wurde.

Tabelle 24. Felder in der Tabelle berechtigter Entitäten

Feld	Beschreibung	Datentyp
auth_entity_id	Die eindeutige interne Kennung der berechtigten Entität.	smallint
auth_entity_desc	Die Kennung der berechtigten Entität, die zur Anzeige genutzt werden kann. In der Regel handelt es sich hierbei um den DN der berechtigten Entität.	varchar
Integrität	Dieses Feld dient der Integrität des Datensatzes.	varchar für Bitdaten

Tabelle der berechtigten Aufgabenbereiche

Diese Tabelle enthält Informationen zu den Aufgabenbereichen berechtigter Entitäten. Diese Tabelle ist schreibgeschützt und wird bei Installation und Konfiguration geladen.

Tabelle 25. Felder in der Tabelle berechtigter Aufgabenbereiche

Feld	Beschreibung	Datentyp
auth_role_id	Die eindeutige interne Kennung des berechtigten Aufgabenbereichs.	smallint
auth_role_desc	Die NLS-Zeichenfolge, die den berechtigten Aufgabenbereich beschreibt.	varchar

Tabelle der Arten betroffener Entitäten

Diese Tabelle enthält Informationen zu verschiedenen Arten betroffener Entitäten. Eine betroffene Entität wird von der Operation beeinflußt, für die ein Prüfereignis erzeugt wird. Diese Tabelle ist schreibgeschützt und wird bei Installation und Konfiguration geladen.

Tabelle 26. Felder in der Tabelle der Arten betroffener Entitäten

Feld	Beschreibung	Datentyp
afctd_entity_id	Die eindeutige interne Kennung der betroffenen Entität.	smallint
afctd_entity_desc	Die NLS-Zeichenfolge, die die betroffene Entität beschreibt.	varchar

Tabelle der Komponentenarten

Diese Tabelle enthält Informationen zu den verschiedenen Komponentenarten des Prüf-Clients. Diese Tabelle ist schreibgeschützt und wird bei Installation und Konfiguration geladen.

Tabelle 27. Felder in der Tabelle der Komponentenarten

Feld	Beschreibung	Datentyp
component_type_id	Die eindeutige interne Kennung der Komponentenart.	smallint
component_desc	Die NLS-Zeichenfolge, die die Komponentenart beschreibt.	varchar

Prüfprotokolltabelle

Diese Tabelle enthält die Protokolleinträge.

Tabelle 28. Felder in der Prüfprotokolltabelle

Feld	Beschreibung	Datentyp
serial_num	Die eindeutige Seriennummer des Protokolleintrags.	smallint
src_date_time	Die Zeitmarke, die angibt, wann das Ereignis von der Quelle (Prüf-Client) erzeugt wurde.	Zeitmarke
cr_date_time	Die Zeitmarke, die angibt, wann der Protokolleintrag vom Prüf-Server erzeugt wurde.	Zeitmarke
event_id	Die interne Ereigniskennung. Dies ist ein fremder Schlüssel, der auf die Tabelle event_ctl verweist.	smallint
source_id	Die interne Kennung der Quelle, die dieses Ereignis erzeugt hat. Dies ist ein fremder Schlüssel, der auf die Quellentabelle verweist.	smallint
component_type_id	Die interne Kennung der Komponentenart der Quelle, die dieses Ereignis erzeugt hat. Dies ist ein fremder Schlüssel, der auf die Tabelle component_types verweist.	smallint
auth_entity_id	Die interne Kennung der Entität, die dieses Ereignis berechtigt hat. Dies ist ein fremder Schlüssel, der auf die Tabelle auth_entities verweist.	smallint
auth_role_id	Die interne Kennung des Aufgabenbereichs der Entität, die dieses Ereignis berechtigt hat. Dies ist ein fremder Schlüssel, der auf die Tabelle auth_entities verweist.	smallint
afctd_entity	Der Name oder DN der Art der Entität, die von diesem Ereignis betroffen ist.	varchar
afctd_entity_id	Die interne Kennung der Art der Entität, die von diesem Ereignis betroffen ist.	smallint
storage_media	Das dem Prüfereignis zugeordnete Speichermedium.	varchar

Tabelle 28. Felder in der Prüfprotokolltabelle (Forts.)

Feld	Beschreibung	Datentyp
extra_info	Dem Prüfereignis zugeordnete Zusatzinformationen.	varchar
sig_key_id	Die interne Kennung des Schlüssels, der zur Erzeugung des Integritätsfelds verwendet wurde. Dies ist ein fremder Schlüssel, der auf die Schlüsseltabelle verweist.	smallint
enc_key_id	Die interne Kennung des Schlüssels, der zur Verschlüsselung ausgewählter Felder des Datensatzes verwendet wird. Dies ist ein fremder Schlüssel, der auf die Schlüsseltabelle verweist. In der aktuellen Version von Trust Authority wird keines der Felder verschlüsselt.	smallint
Integrität	Dieses Feld dient der Aufrechterhaltung der Integrität des Datensatzes.	varchar für Bitdaten

Systemtabelle

Diese Tabelle enthält Statusinformationen zur Prüfdatenbank.

Tabelle 29. Felder in der Systemtabelle

Feld	Beschreibung	Datentyp
first_sn	Die Seriennummer des ersten Protokolleintrag in audit_log.	integer
next_sn	Die Seriennummer des nächsten Protokolleintrags in audit_log.	integer
audit_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle audit_log.	varchar für Bitdaten
archive_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle archive_ctl.	varchar für Bitdaten
events_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle events_ctl.	varchar für Bitdaten
auth_ent_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle auth_entities.	varchar für Bitdaten
auth_role_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle auth_roles.	varchar für Bitdaten

Tabelle 29. Felder in der Systemtabelle (Forts.)

Feld	Beschreibung	Datentyp
sources_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Quellentabelle.	varchar für Bitdaten
afctd_ent_type_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle afctd_entities.	varchar für Bitdaten
keys_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Schlüsseltabelle.	varchar für Bitdaten
event_sevs_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle der Ereignisbewertung.	varchar für Bitdaten
comp_types_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Tabelle der Komponententarten.	varchar für Bitdaten
system_int	Dieses Feld dient der Aufrechterhaltung der Integrität der Systemtabelle.	varchar für Bitdaten
sig_key_id	Die interne Kennung des Schlüssels, der zur Erzeugung der Integritätsfelder dieses Datensatzes verwendet wird. Dies ist ein fremder Schlüssel, der auf die Schlüsseltabelle verweist.	smallint

Fehlerbehebung

Bei der Standardinstallation von Trust Authority werden keine Protokolldateien für die ausführliche Stufe bzw. Debug-Stufe von Fehlernachrichten erstellt. Dieser Abschnitt beschreibt die Basisschritte zur Fehlerbehebung, wobei die Nachrichtenerstellung auf Debug-Stufe inaktiviert ist. Wenn Sie ausführlichere Informationen benötigen, können Sie die Debug-Nachrichtenerstellung mit Hilfe der unter „Fehlerbehebung mit aktivierter Nachrichtenerstellung auf Debug-Stufe" auf Seite 121 beschriebenen Prozedur aktivieren.

Grundlegende Fehlerbehebung

Befolgen Sie die nachfolgenden Anweisungen, um Probleme bei der Verwaltung von Trust Authority zu beheben:

1. Stoppen Sie das Trust Authority-System.
2. Führen Sie einen Warmstart durch.
3. Starten Sie das Trust Authority-System.
4. Prüfen Sie den Status aller Komponenten, um den korrekten Betrieb zu gewährleisten.
5. Reproduzieren Sie das Problem, und prüfen Sie die Protokolle aller Komponenten, um den Fehler zu lokalisieren.

Fehlerbehebung mit aktivierter Nachrichtenerstellung auf Debug-Stufe

Wenn Sie bei einem Fehler ausführliche Unterstützung zur Fehlerbehebung benötigen, aktivieren Sie die Umgebungsvariable für die Debug-Stufe (DebugLevel). Sie können diesen Wert Ihren Bedürfnissen entsprechend anpassen, je nachdem, ob Sie mehr oder weniger Nachrichtendetails erhalten wollen. Die in dieser Variable angegebene Protokollstufe legt den Protokollumfang fest. Der Wert ist eine positive ganze Zahl im Bereich zwischen 0 und 1000. Je höher die Stufe, desto umfangreicher die Protokollierung. Die folgenden Trust Authority-Debug-Stufen werden empfohlen:

- DebugLevel=25 - Minimale Protokollierung; es werden jedoch alle Fehler aufgezeichnet.

  Verwenden Sie diese Stufe für ständige Operationen, bei denen Probleme zwar nicht aktiv diagnostiziert werden, bei denen Sie die Protokolle jedoch gegebenenfalls einsehen wollen, falls doch etwas passiert.
- DebugLevel=75 - Enthält zusätzlich die Protokollierung von darunter liegenden Softwareschichten.

  Verwenden Sie diese Stufe, wenn Probleme zwischen den CA- und RA-Servern auftreten. Das Ausgabevolumen ist etwa fünfmal höher als bei Debug-Stufe 25.
- DebugLevel=101 - Enthält eine umfangreiche und detaillierte Protokollierung der höherstufigen RA-Server-Verarbeitung, einschließlich der Verarbeitung von Zertifikatsprofilen und der AFW-Interaktionen (Application Framework = Anwendungsgerüst).

  Verwenden Sie diese Stufe, wenn Sie versuchen, Probleme in den Schichten des RA-Servers für die Zertifikatsverarbeitung zu diagnostizieren. Das Ausgabevolumen ist etwa zehnmal höher als bei Debug-Stufe 25.
- DebugLevel=201 - Umfangreiche Ablaufverfolgung (Tracing) kritischer, interner Funktionen, die sehr häufig verwendet werden.

  Verwenden Sie diese Stufe nur dann, wenn Sie versuchen, Probleme wie abnormale Beendigungen des RA-Servers zu diagnostizieren. Das Ausgabevolumen ist etwa hundertmal höher als bei Debug-Stufe 25.

Anmerkung: Aufgrund des hohen Protokollvolumens auf Stufe 100 sollten Sie diese Einstellung nicht in einer Produktionsumgebung verwenden, sofern keine besonderen Umstände vorliegen. Auf dieser oder einer höheren Debug-Stufe besteht die Möglichkeit, daß der freie Speicherplatz im Dateisystem aufgebraucht wird, was zu zahlreichen Störungen im gesamten System führen kann.

Um die Fehlerbehebung mit aktivierter Nachrichtenerstellung auf Debug-Stufe auszuführen, gehen Sie folgendermaßen vor (bei dieser Prozedur wird als Beispiel die Debug-Stufe 100 verwendet):

1. Stoppen Sie das Trust Authority-System.
2. Ändern Sie die Datei 'irgAutoCa.ini' folgendermaßen:
   - Unter AIX: Geben Sie für den Debug-Parameter in `/usr/lpp/iau/etc/TrustAuthority/irgAutoCa.ini` einen Wert zwischen 50 und 100 an.
   - Unter Windows NT: Geben Sie für den Debug-Parameter in `C:\Program Files\IBM\Trust Authority\etc\TrustAuthority\irgAutoCa.ini` einen Wert zwischen 50 und 100 an.
3. Aktivieren Sie folgendermaßen die Umgebungsvariable für die Debug-Stufe (DebugLevel):
   - Unter AIX: Geben Sie den folgenden Befehl in die Befehlszeile der Maschine ein, auf der sich der RA-Server befindet:

     ```
     export DebugLevel=
     ```

   - Unter Windows NT:
     a. Rufen Sie die Systemeigenschaften auf, indem Sie mit der rechten Maustaste auf das Symbol **Arbeitsplatz** im Windows NT Explorer klicken und **Eigenschaften** auswählen.
     b. Klicken Sie auf die Registerkarte **Umgebung**.
     c. Geben Sie **`DebugLevel`** in das Feld **Variable** und **`100`** in das Feld **Wert** ein.
     d. Klicken Sie auf **Setzen** und anschließend auf **Übernehmen**.
     e. Klicken Sie auf **OK**, um das Fenster mit den Systemeigenschaften zu schließen.
4. Starten Sie das Trust Authority-System.
5. Prüfen Sie den Status aller Komponenten, um den korrekten Betrieb zu gewährleisten.
6. Reproduzieren Sie das Problem, und prüfen Sie die Protokolle aller Komponenten, um den Fehler zu lokalisieren.

   Es werden Protokolldateien mit dem Dateinamen 'irgrasvr.log.*nnnn*' erstellt, wobei *nnnn* eine nach dem Zufallsprinzip generierte Zahl ist.
   - Unter AIX ist die Standardposition der Protokolldateien /usr/lpp/iau/etc/TrustAuthority/caSS.log.xxxxx.
   - Unter Windows NT ist die Standardposition c:\Program Files\IBM\Trust Authority\etc\TrustAuthority\caSS.log.xxxxx.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb der Produkte, Programme und Dienstleistungen in Verbindung mit Fremdprodukten liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich von IBM bestätigt sind.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf englisch formuliert werden.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Änderung des Textes bleibt vorbehalten.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne daß eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäfts-

bedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Garantie, daß diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen. Diese Daten stellen deshalb keine Leistungsgarantie dar.

Informationen über Produkte anderer Hersteller als IBM wurden von den Herstellern dieser Produkte zur Verfügung gestellt, bzw. aus von ihnen veröffentlichten Ankündigungen oder anderen öffentlich zugänglichen Quellen entnommen. IBM hat diese Produkte nicht getestet und übernimmt im Hinblick auf Produkte anderer Hersteller keine Verantwortung für einwandfreie Funktion, Kompatibilität oder andere Ansprüche. Fragen hinsichtlich des Leistungsspektrums von Produkten anderer Hersteller als IBM sind an den jeweiligen Hersteller des Produkts zu richten.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht der IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele der IBM.

Alle von IBM angegebenen Preisen sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Marken und Dienstleistungsmarken

Folgende Namen sind in gewissen Ländern Marken der IBM Corporation:

IBM
AIX
AIX/6000
DB2
DB2 Universal Database
RS/6000
SecureWay
WebSphere

Das Programm Trust Authority (im folgenden als ″Programm″ bezeichnet) enthält Komponenten von DB2 Universal Database. Diese Komponenten dürfen nur zusammen mit dem Programm installiert und entsprechend der für das Programm geltenden Lizenzvereinbarungen in Kombination mit diesem verwendet werden, um Daten zu speichern und zu verwalten, die vom Programm verwendet oder generiert werden. Für andere Datenverwaltungsoperationen ist der Einsatz nicht gestattet. Diese Lizenz gilt z. B. nicht für eingehende Verbindungen zur Datenbank, die von anderen Anwendungen aus für Abfragen und Berichtserstellungsoperationen hergestellt werden. Sie sind lediglich zur Installation und Verwendung dieser Komponenten auf der gleichen Maschine berechtigt, auf der auch das Programm installiert und verwendet wird.

Das Programm enthält Komponenten des IBM WebSphere Application Server und des IBM HTTP Web Server (″IBM Server″). Sie sind nicht berechtigt, die IBM Server zu anderen Zwecken als in Verbindung mit der lizenzgerechten Verwendung des Programms zu benutzen. Die IBM Server müssen auf derselben Maschine wie das Programm installiert sein. Sie sind nicht berechtigt, sie unabhängig vom Programm zu installieren und zu verwenden.

Java und alle auf Java basierenden Marken und Logos sind in gewissen Ländern Marken der Sun Microsystems, Inc.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

UNIX ist eine eingetragene Marke und wird ausschließlich von der X/Open Company Limited lizenziert.

Pentium ist in gewissen Ländern eine Marke der Intel Corporation.

Dieses Programm enthält Sicherheitssoftware von RSA Data Security, Inc. Copyright © 1994 RSA Data Security, Inc. Alle Rechte vorbehalten.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Hewlett-Packard Company. Copyright (c) 1994.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Hewlett-Packard Company macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Silicon Graphics Computer Systems, Inc. Copyright (c) 1996 - 1999.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Silicon Graphics macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken anderer Unternehmen sein.

Bezugsinformationen

Die Produktdokumentation zu Trust Authority ist auf der CD-ROM *IBM SecureWay Trust Authority-Dokumentation* im PDF- (Portable Document Format) und HTML-Format verfügbar. Die HTML-Versionen einiger Veröffentlichungen sind mit dem Produkt installiert und können über die Benutzerschnittstelle abgerufen werden.

Bitte beachten Sie, daß seit der Produktion der Dokumentation eventuell Änderungen am Produkt vorgenommen wurden. Aktuelle Produktinformationen sowie Informationen für den Zugriff auf Veröffentlichungen in der Sprache und im Format Ihrer Wahl finden Sie in der Informationsdatei (*Readme*). Die neueste Version der *Readme*-Datei steht auf der folgenden Web-Site von IBM SecureWay Trust Authority zur Verfügung:

`http://www.tivoli.com/support`

Die Trust Authority-Bibliothek umfaßt folgende Dokumentation:

Einführung
: Dieses Handbuch enthält eine Produktübersicht, führt die Produktvoraussetzungen und Installationsverfahren auf und bietet Informationen zum Zugriff auf die verfügbare Online-Hilfe für jede Produktkomponente. Dieses Buch liegt in gedruckter Form vor und wird mit dem Produkt geliefert.

Systemverwaltung
: Dieses Handbuch enthält Basisinformationen zur Verwaltung des Trust Authority-Systems. Es beschreibt die Prozeduren zum Starten und Stoppen der Server, zum Ändern von Kennwörtern, zur Verwaltung der Server-Komponenten sowie zum Erstellen von Protokollen und zur Ausführung von Datenintegritätsüberprüfungen.

Konfiguration
: Dieses Handbuch enthält Informationen zur Verwendung des Setup Wizard für die Konfiguration eines Trust Authority-Systems. Sie können auf die HTML-Version dieses Handbuchs zugreifen, während Sie die Online-Hilfe des Wizards nutzen.

Registration Authority Desktop
: Dieses Handbuch enthält Informationen zur Verwendung von RA Desktop für die Verwaltung von Zertifikaten während ihres Gültigkeitszeitraums. Sie können auf die HTML-Version dieses Handbuchs zugreifen, während Sie die Online-Hilfe des Desktops nutzen.

Benutzerhandbuch
: Dieses Buch enthält Informationen darüber, wie Zertifikate abgerufen und verwaltet werden. Es beschreibt die Prozeduren zur Verwendung der Browser-Registrierungsformulare von Trust Authority, um Zertifikate anzufordern, zu erneuern und zu widerrufen. Außerdem beschreibt das Buch, wie eine Vorabregistrierung für PKIX-kompatible Zertifikate durchgeführt wird und wie diese Zertifikate mit Hilfe des Trust Authority Client verwaltet werden. Sie können auf die HTML-Version dieses Handbuchs zugreifen, während Sie die Online-Hilfe für den Client nutzen.

Anpassung

Dieses Buch zeigt, wie die Trust Authority-Registrierungsfunktion angepaßt wird, um die Vorgaben zur Registrierung und Zertifizierung im Rahmen Ihrer Geschäftsregeln zu unterstützen. Sie erfahren beispielsweise, wie HTML- und Java Server-Seiten, Mitteilungsschreiben, Zertifikatsprofile und Regel-Exits angepaßt werden.

Die Trust Authority-Web-Site enthält weitere Dokumente, die Ihnen bei der Installation, Verwaltung un Nutzung von Trust Authority helfen können. Dort finden Sie beispielsweise zusätzliche Richtlinien zum Directory-Schema und erfahren, wie Trust Authority in den IBM SecureWay 4758 PCI Cryptographic Coprocessor integriert wird.

Glossar

In diesem Glossar werden alle Termini und Abkürzungen definiert, die in diesem Handbuch verwendet werden und die möglicherweise neu oder unbekannt und von Bedeutung sind.

Numerische Einträge

4758 PCI Cryptographic Coprocessor. Eine programmierbare, manipulationssensitive PCI-Bus-Verschlüsselungskarte, die die Ausführung von DES- und RSA-Verschlüsselungsoperationen mit hoher Geschwindigkeit ermöglicht. Die Verschlüsselungsprozesse werden in einem gesicherten und abgegrenzten Bereich auf der Karte ausgeführt. Die Karte entspricht den strengen Anforderungen des FIPS PUB 140-1 Level 4-Standards. In dem gesicherten und abgegrenzten Bereich kann Software ausgeführt werden. Der SET-Standard kann z. B. zur Verarbeitung von Kreditkartentransaktionen genutzt werden.

A

Abstract Syntax Notation One (ASN.1). Eine ITU-Notation, die zum Definieren der Syntax von Informationsdaten benutzt wird. Sie definiert eine Reihe einfacher Datentypen und gibt eine Notation für die Identifizierung dieser Typen und die Angabe von Werten für diese Typen an. Diese Notationen können verwendet werden, wenn es erforderlich ist, die abstrakte Syntax von Informationen zu definieren, ohne damit die Art der Verschlüsselung dieser Informationen für die Übertragung zu beeinträchtigen.

ACL. Access Control List - Zugriffssteuerungsliste.

Aktionsprotokoll. Die Aufzeichnung aller Ereignisse, die während der gesamten Gültigkeitsdauer eines Identitätsnachweises aufgetreten sind.

American National Standard Code for Information Interchange (ASCII). Der Standardcode, der für den Austausch von Informationen zwischen Datenverarbeitungssystemen, DFV-Systemen und zugehöriger Hardware verwendet wird. ASCII verwendet einen codierten Zeichensatz, der aus Zeichen von 7 Bit Länge (bzw. 8 Bit bei Paritätsprüfung) besteht. Der Zeichensatz besteht hierbei aus Steuerzeichen und Schriftzeichen.

American National Standards Institute (ANSI). Eine Organisation, die die Verfahrensweisen definiert, mit deren Hilfe akkreditierte Organisationen freiwillig eingehaltene Industriestandards in den Vereinigten Staaten festlegen und verwalten. Ihr gehören Hersteller, Verbraucher und allgemeine Interessenvertretungen an.

Anforderungs-ID. Ein aus 24 bis 32 Zeichen bestehender ASCII-Wert, der zur eindeutigen Identifikation einer Zertifikatsanforderung gegenüber der RA dient. Dieser Wert kann bei der Transaktion für die Zertifikatsanforderung verwendet werden, um den Status der Anforderung oder des zugehörigen Zertifikats abzurufen.

ANSI. American National Standards Institute.

Applet. Ein in der Programmiersprache Java geschriebenes Computerprogramm, das innerhalb eines Java-kompatiblen Web-Browsers ausgeführt werden kann. Dieses wird auch als Java-Applet bezeichnet.

Art. *Siehe* Objektart.

ASCII. American National Standard Code for Information Interchange.

ASN.1. Abstract Syntax Notation One.

Asymmetrische Verschlüsselung. Ein Verschlüsselungsverfahren, das zur Ver- und Entschlüsselung unterschiedliche, asymmetrische Schlüssel verwendet. Jedem Benutzer wird hierbei ein Schlüsselpaar zugeordnet, das einen allgemeinen, für alle zugänglichen Schlüssel und einen privaten Schlüssel umfaßt, der nur dem jeweiligen Benutzer bekannt ist. Eine gesicherte Transaktion kann ausgeführt werden, wenn der öffentliche Schlüssel sowie der zugehörige private Schlüssel übereinstimmen. In diesem Fall kann die Transaktion entschlüsselt werden. Dieses Verfahren wird auch als Verschlüsselung auf der Basis von Schlüsselpaaren bezeichnet. *Gegensatz zu* Symmetrische Verschlüsselung.

Asynchrone Übertragung. Ein Übertragungsmodus, bei dem Sender und Empfänger nicht gleichzeitig vorhanden sein müssen.

Authentifizierung. Der Vorgang, bei dem die Identität eines Teilnehmers an einer Übertragung zuverlässig überprüft wird.

B

Base64-Verschlüsselung. Ein häufig verwendetes Verfahren bei der Übertragung von Binärdaten mit MIME.

Basic Encoding Rules (BER). Die Regeln, die in ISO 8825 für die Verschlüsselung von in ASN.1 beschriebenen Dateneinheiten angegeben sind. Die Regeln geben das Verschlüsselungsverfahren, jedoch nicht die abstrakte Syntax an.

Benutzerauthentifizierung. Der Prozeß, mit dem überprüft wird, ob der Absender einer Nachricht die berechtigte Person ist, als die er sich ausgibt. Der Prozeß überprüft außerdem, ob ein Kommunikationsteilnehmer auch tatsächlich mit dem erwarteten Endbenutzer oder System in Verbindung steht.

BER. Basic Encoding Rules.

Berechtigung. Die Erlaubnis, auf eine Ressource zuzugreifen.

Bestreiten. Etwas als unwahr zurückweisen. Dies ist z. B. dann der Fall, wenn ein Benutzer abstreitet, eine bestimmte Nachricht gesendet oder eine bestimmte Anforderung übergeben zu haben.

Browser. *Siehe* Web-Browser.

Browser-Zertifikat. Ein digitales Zertifikat, das auch als Zertifikat der Client-Seite bezeichnet wird. Es wird von einem CA über einen für SSL aktivierten Web-Server ausgestellt. Die Schlüssel in einer verschlüsselten Datei ermöglichen dem Inhaber des Zertifikats das Verschlüsseln, Entschlüsseln und Unterzeichnen von Daten. Normalerweise werden diese Schlüssel im Web-Browser gespeichert. In bestimmten Anwendungen können die Schlüssel auf Smart-Cards oder anderen Speichermedien gespeichert werden. *Siehe auch* Digitales Zertifikat.

Bytecode. Maschinenunabhängiger Code, der mit dem Java-Compiler generiert und mit dem Java-Interpreter ausgeführt wird.

C

CA. Certificate Authority - Zertifikatsaussteller.

CA-Hierarchie. Bei Trust Authority eine Sicherungsstruktur, bei der ein CA auf der höchsten Ebene positioniert ist. Anschließend können bis zu vier weitere Ebenen mit untergeordneten CAs definiert werden. Wenn Benutzer oder Server bei einem Zertifikatsaussteller registriert werden, wird ihnen ein von diesem Aussteller unterzeichnetes Zertifikat zugeordnet. Außerdem übernehmen sie die Zertifizierungshierarchie der übergeordneten Ebenen.

CA-Server. Der Server für die CA-Komponente von Trust Authority.

CA-Zertifikat. Ein Zertifikat, das vom Web-Browser eines Benutzers auf dessen Anforderung hin von einem nicht identifizierten CA akzeptiert wird. Der Browser kann dann dieses Zertifikat verwenden, um für die Kommunikation mit Servern, die über Zertifikate dieses CAs verfügen, eine Authentifizierung durchzuführen.

CAST-64. Ein Block-Cipher-Algorithmus, der mit einer Blockgröße von 64 Bit und einem 6-Bit-Schlüssel arbeitet. Er wurde von Carlisle Adams und Stafford Tavares entwickelt.

CCA. Common Cryptographic Architecture.

CDSA. Common Data Security Architecture.

CGI. Common Gateway Interface.

Client. (1) Eine Funktionseinheit, die gemeinsam benutzte Services von einem Server empfängt. (2) Ein Computer oder Programm, der/das Services von einem anderen Computer oder Programm anfordert.

Client/Server. Ein Modell für die verteilte Verarbeitung, bei dem ein Programm an einem Standort eine Anforderung an ein Programm an einem anderen Standort sendet und auf eine Antwort wartet. Das anfordernde Programm wird als Client, das antwortende als Server bezeichnet.

Codeunterzeichnung. Ein Verfahren zum Unterzeichnen ausführbarer Programme mit einer digitalen Unterschrift. Die Codeunterzeichnung dient zur Verbesserung der Zuverlässigkeit von Softwarekomponenten, die über das Internet verteilt werden.

Common Cryptographic Architecture (CCA). IBM Software, die einen konsistenten Verschlüsselungsansatz auf den wichtigsten IBM Computerplattformen bietet. Sie unterstützt Anwendungssoftware, die in einer Vielzahl von Programmiersprachen geschrieben wurde. Die Anwendungssoftware kann hierbei die CCA-Services aufrufen, um eine breite Palette kryptografischer Funktionen (einschließlich der DES- und der RSA-Verschlüsselung) auszuführen.

Common Data Security Architecture (CDSA). Eine Initiative zum Definieren eines umfassenden Ansatzes für Sicherheitsservices und Sicherheitsverwaltungsoperationen bei computerbasierten Sicherheitsanwendungen. Diese Architektur wurde von Intel entworfen und dient dazu, Computerplattformen für Anwendungen sicherer zu gestalten.

Common Gateway Interface (CGI). Ein Standardverfahren zum Übertragen von Informationen zwischen Web-Seiten und Web-Servern.

CRL. Certificate Revocation List - Zertifikatswiderrufsliste.

CRL-Veröffentlichungsintervall. Dieses Intervall wird in der CA-Konfigurationsdatei definiert und gibt das Zeitintervall zwischen zwei Veröffentlichungen der Zertifikatswiderrufsliste im Directory an.

D

Dämon. Ein Programm, das Tasks im Hintergrund ausführt. Es wird implizit aufgerufen, wenn eine Bedin-

gung auftritt, die die Hilfe des Dämons erforderlich macht. Es ist nicht erforderlich, daß der Benutzer über die Ausführung des Dämons unterrichtet wird, da der Dämon normalerweise vom System automatisch gestartet wird. Ein Dämon kann über eine unbegrenzte Zeit hinweg ausgeführt oder vom System in bestimmten Zeitintervallen erneut generiert werden.

Der Terminus (englisch *demon*) stammt aus der Mythologie. Später wurde er aber als Akronym für den Ausdruck "Disk And Execution MONitor" (Platten- und Ausführungsüberwachungsprogramm) erklärt.

Data Encryption Standard (DES). Eine Verschlüsselungs-Block-Cipher, die 1977 von der US-Regierung als offizieller Standard definiert und übernommen wurde. Dieser Standard wurde ursprünglich von IBM entwickelt. DES wurde seit seiner Veröffentlichung umfassend untersucht und stellt ein allgemein bekanntes und häufig verwendetes Verschlüsselungssystem zur Verfügung.

Bei DES handelt es sich um ein symmetrisches Verschlüsselungssystem. Um es für die Datenübertragung einzusetzen, müssen sowohl der Sender als auch der Empfänger den selben, geheimen Schlüssel kennen. Dieser Schlüssel wird zum Ver- und Entschlüsseln der Nachricht verwendet. DES kann außerdem zur Durchführung von Verschlüsselungsoperationen für einzelne Benutzer eingesetzt werden, z. B. zum Speichern von verschlüsselten Dateien auf einer Festplatte. DES arbeitet mit einer Blockgröße von 64 Bit und verwendet für die Verschlüsselung einen 56-Bit-Schlüssel. Ursprünglich wurde dieser Standard für die Hardwareimplementierung entwickelt. DES wird von NIST alle fünf Jahre erneut als offizieller Verschlüsselungsstandard der US-Regierung zertifiziert.

Datenspeicherbibliothek (DL). Ein Modul, das den Zugriff auf permanente Datenspeicher mit Zertifikaten, CRLs, Schlüsseln, Regeln und anderen sicherheitsrelevanten Objekten ermöglicht.

DEK. Document Encryption Key = Dokumentverschlüsselungsschlüssel.

DER. Distinguished Encoding Rules.

DES. Data Encryption Standard.

Diffie-Hellman. Ein Verfahren zur Datenverschlüsselung, das auf der Verwendung eines gemeinsamen Schlüssels auf einem nicht gesicherten Medium basiert und nach seinen Erfindern (Whitfield Diffie und Martin Hellman) benannt wurde.

Digital Signature Algorithm (DSA). Ein auf öffentlichen Schlüsseln basierender Algorithmus, der zum Standard für digitale Unterschriften (Digital Signature Standard = DSS) gehört. Er kann nur für digitale Unterschriften, jedoch nicht für die Verschlüsselung verwendet werden.

Digitale Unterschrift. Eine codierte Nachricht, die an Dokumente oder Daten angefügt wird, und die Identität des Absenders nachweist.

Eine digitale Unterschrift gewährleistet ein höheres Maß an Sicherheit als eine physische Unterschrift, da es sich hierbei nicht lediglich um einen verschlüsselten Namen oder eine Reihe einfacher Identifikationscodes handelt. Eine digitale Unterschrift enthält eine verschlüsselte Zusammenfassung der unterzeichneten Nachricht. Durch das Anfügen einer digitalen Unterschrift an eine Nachricht läßt sich der Absender also zweifelsfrei feststellen. (Die Unterschrift kann nur mit Hilfe des Schlüssels des Absenders erstellt werden.) Außerdem ermöglicht sie die Absicherung des Inhalts der unterzeichneten Nachricht, da die verschlüsselte Nachrichtenzusammenfassung mit dem Nachrichteninhalt übereinstimmen muß. Andernfalls wird die Unterschrift nicht als gültig identifiziert. Eine digitale Unterschrift kann also nicht von einer Nachricht kopiert und für eine andere Nachricht verwendet werden, da sonst die Zusammenfassung (Hash-Code) nicht übereinstimmen würde. Alle Änderungen an der unterzeichneten Nachricht führen automatisch zum Verlust der Gültigkeit der Unterschrift.

Digitale Zertifizierung. *Siehe* Zertifizierung.

Digitales Zertifikat. Ein elektronischer Identitätsnachweis, der von einer zuverlässigen Stelle für eine Person oder Entität ausgestellt wird. Jedes Zertifikat ist mit dem privaten Schlüssel des CAs unterzeichnet. Es bürgt für die Identität einer Person, eines Unternehmens oder einer Organisation.

Abhängig vom Aufgabenbereich des CAs kann das Zertifikat die Berechtigung seines Inhabers bestätigen, e-Business-Transaktionen über das Internet auszuführen. In gewisser Weise hat ein digitales Zertifikat eine ähnliche Funktion wie ein Führerschein oder ein Meisterbrief. Es bestätigt, daß der Inhaber des entsprechenden privaten Schlüssels berechtigt ist, bestimmte e-Business-Aktivitäten auszuführen.

Ein Zertifikat enthält Informationen über die Entität, die von ihm zertifiziert wird, gibt an, ob es sich um eine Person, eine Maschine oder ein Computerprogramm handelt und enthält als Teil dieser Informationen den zertifizierten öffentlichen Schlüssel dieser Entität.

Directory. Eine hierarchische Struktur, die als globales Repository für Informationen zur Datenkommunikation (wie beispielsweise E-Mail oder Austausch von verschlüsselten Daten) konzipiert ist. Im Directory werden bestimmte Elemente gespeichert, die für die PKI-Struktur (PKI = Public Key Infrastructure) unbedingt erforderlich sind. Hierzu gehören die folgenden Elemente: öffentliche Schlüssel, Zertifikate und Zertifikatswiderrufslisten (CRLs).

Die Daten im Directory sind hierarchisch in einer Baumstruktur organisiert, wobei die oberste Ebene der Baumstruktur das Root-Verzeichnis ist. Häufig stehen

Organisationen einer höheren Ebene für einzelne Länder, Regierungen oder Unternehmen. Benutzer oder Einheiten werden im allgemeinen als ″Blätter″ einer solchen Baumstruktur dargestellt. Diese Benutzer, Organisationen, Standorte, Länder und Einheiten haben jeweils ihren eigenen Eintrag. Jeder Eintrag besteht aus Attributen, denen verschiedene Typen zugewiesen sind. Diese enthalten Informationen zu den Objekten, für die der jeweilige Eintrag steht.

Jeder Eintrag im Directory ist mit einem zugeordneten registrierten Namen (DN = Distinguished Name) verbunden. Dieser ist eindeutig, wenn der Eintrag ein Attribut umfaßt, das für das tatsächliche Objekt als eindeutig bekannt ist. Im folgenden DN-Beispiel wurde als Land (C = Country) US, als Unternehmen (O = Organization) IBM, als Unternehmenseinheit (OU = Organization Unit) Trust und als allgemeiner Name (CN = Common Name) der Wert CA1 angegeben.

```
C=US/O=IBM/OU=Trust/CN=CA1
```

Directory-Server. Unter Trust Authority das IBM SecureWay Directory. Dieses Directory unterstützt die LDAP-Standards und verwendet DB2 als Basissystem.

Distinguished Encoding Rules (DER). Durch DER werden bestimmte Einschränkungen für BER definiert. Mit DER kann genau ein bestimmter Verschlüsselungstyp aus den verfügbaren und auf der Basis der Verschlüsselungsregeln als zulässig definierten Typen ausgewählt werden. Hierdurch werden alle Senderoptionen eliminiert.

DL. Data Storage Library = Datenspeicherbibliothek.

DN. Distinguished Name - Registrierter Name.

Dokumentverschlüsselungsschlüssel (DEK). Normalerweise ein symmetrischer Ver-/Entschlüsselungsschlüssel, z. B. DES.

Domäne. *Siehe* Sicherheitsdomäne *und* Registrierungsdomäne.

DSA. Digital Signature Algorithm.

E

e-Business. Das Durchführen geschäftlicher Transaktionen über Netze und Computer, z. B. der Kauf und Verkauf von Waren und Dienstleistungen sowie der Transfer von Zahlungsmitteln mit Hilfe der digitalen Kommunikation.

e-Commerce. Unternehmensübergreifende Transaktionen wie beispielsweise der Kauf und Verkauf von Waren und Dienstleistungen (zwischen Unternehmen und ihren Kunden, Lieferanten, Subunternehmen und anderen) über das Internet. E-Commerce stellt einen Kernbestandteil des e-Business dar.

Endentität. Der Gegenstand eines Zertifikats, bei dem es sich nicht um einen CA handelt.

Entschlüsseln. Den Verschlüsselungsprozeß rückgängig machen.

Exemplar. Bei DB2 bezeichnet man als Exemplar eine logische Datenbankverwaltungsumgebung zum Speichern von Daten und Ausführen von Anwendungen. Es ermöglicht die Definition einer allgemeinen Gruppe von Konfigurationsparametern für verschiedene Datenbanken.

Extranet. Ein Netz, das auf dem Internet basiert und eine ähnliche Technologie einsetzt. Unternehmen beginnen momentan mit dem Einsatz des Web Publishings, elektronischen Handels und der Nachrichtenübertragung sowie der Verwendung von Groupware für verschiedene Gruppen von Kunden, Partnern und internen Mitarbeitern.

F

File Transfer Protocol (FTP). Ein Client/Server-Protokoll im Internet, das zum Übertragen von Dateien zwischen Computern benutzt wird.

Firewall. Ein Gateway zwischen Netzen, der den Informationsfluß zwischen diesen einschränkt. Normalerweise dienen Firewalls dem Schutz interner Netze gegen die nicht berechtigte Verwendung durch externe Personen.

FTP. File Transfer Protocol.

G

Gateway. Eine Funktionseinheit, mit deren Hilfe nicht kompatible Netze oder Anwendungen Daten austauschen können.

Gegenseitige Zertifizierung. Ein Trust-Modell, bei dem ein CA für einen anderen CA ein Zertifikat ausstellt, das den öffentlichen Schlüssel enthält, der dem entsprechenden privaten Unterschriftsschlüssel zugeordnet ist. Ein gegenseitig zertifiziertes Zertifikat ermöglicht Client-Systemen oder Endentitäten in einer Verwaltungsdomäne die sichere Kommunikation mit Client-Systemen oder Endentitäten in einer anderen Domäne.

Gesicherte Computerbasis (TCB). Die Software- und Hardwareelemente, die zur Umsetzung der Computersicherheitsregeln eines Unternehmens verwendet werden. Alle Elemente oder Teilelemente, die zur Implementierung der Sicherheitsregeln eingesetzt werden können, sind sicherheitsrelevant und Bestandteil der TCB. Bei der TCB handelt es sich um ein Objekt, das durch die Sicherheitsperipherie begrenzt wird. Die Mechanismen, die zur praktischen Umsetzung der Sicherheitsregeln eingesetzt werden, dürfen nicht umgangen werden können und müssen verhindern, daß Programme Zugriff auf Systemprivilegien erlangen können, für die sie nicht berechtigt sind.

H

Höchster CA. Der CA, der innerhalb der PKI-CA-Hierarchie die höchste Position einnimmt.

HTML. Hypertext Markup Language.

HTTP. Hypertext Transaction Protocol.

HTTP-Server. Ein Server, der die Web-gestützte Kommunikation mit Browsern und anderen Programmen im Netz steuert.

Hypertext. Textsegmente, die einzelne oder mehrere Wörter umfassen oder Bilder enthalten, auf die der Leser mit der Maus klicken kann, um ein anderes Dokument aufzurufen und anzuzeigen. Diese Textsegmente werden als Hyperlinks bezeichnet. Ruft der Leser diese anderen Dokumente auf, stellt er zu diesen eine Hyperlink-Verbindung her.

Hypertext Markup Language (HTML). Eine Formatierungssprache für das Codieren von Web-Seiten. HTML basiert auf SGML (Standard Generalized Markup Language).

Hypertext Transaction Protocol (HTTP). Ein Client/Server-Protokoll für das Internet, mit dem Hypertext-Dateien im Web übertragen werden.

I

ICL. Issued Certificate List - Liste der ausgestellten Zertifikate.

Identitätsnachweis. Vertrauliche Informationen, die verwendet werden, um beim Austausch von Daten während der Authentifizierung die eigene Identität zu belegen. In Network Computing-Umgebungen ist die am häufigsten verwendete Form des Identitätsnachweises ein Zertifikat, das von einem CA erstellt und unterzeichnet wurde.

IniEditor. Bei Trust Authority ein Tool, mit dem Konfigurationsdateien editiert werden können.

Integrität. Ein System schützt seine Datenintegrität, wenn es die Änderung dieser Daten durch nicht berechtigte Personen verhindert. (Im Gegensatz hierzu versteht man unter dem Schutz der Vertraulichkeit von Daten, wenn verhindert wird, daß diese unberechtigten Personen zugänglich gemacht werden.)

Integritätsprüfung. Die Prüfung der Protokolleinträge, die für Transaktionen mit externen Komponenten aufgezeichnet wurden.

International Standards Organization (ISO). Eine internationale Organisation, die Standards für eine breite Palette von Industriebereichen, z. B. auch für Computernetzprotokolle, entwickelt und veröffentlicht.

International Telecommunication Union (ITU). Eine internationale Organisation, in der Verwaltungs- und private Industriebereiche globale Datenfernübertragungsnetze und -services koordinieren. Bei der Veröffentlichung von Informationen zur Datenfernübertragungstechnologie sowie den entsprechenden Regelwerken und Standards nimmt sie eine führende Position ein.

Interne Struktur. *Siehe* Schema.

Internet. Ein weltweiter Verbund von Netzen, die die elektronische Verbindung zwischen Computern und die Kommunikation zwischen den Computern über Softwareeinrichtungen wie elektronische Post (E-Mail) oder Web-Browser ermöglichen. So sind beispielsweise die meisten Universitäten in ein Netz eingebunden, das seinerseits eine Verbindung zu anderen ähnlichen Netzen hat, die zusammen das Internet bilden.

Internet Engineering Task Force (IETF). Eine Gruppe, die sich schwerpunktmäßig mit dem Entwickeln und Definieren von Protokollen für das Internet befaßt. Sie repräsentiert eine internationale Gruppe von Netzdesignern, -bedienern, -herstellern und -forschern. Die Aufgabe der IETF ist die Entwicklung der Internet-Architektur sowie die Gewährleistung der reibungslosen Verwendung des Internets.

Intranet. Ein Netz innerhalb eines Unternehmens, das sich im allgemeinen hinter Firewalls befindet. Es basiert auf dem Internet und setzt eine ähnliche Technologie ein. Vom technischen Standpunkt aus ist ein Intranet eine Erweiterung des Internets. Zu den in beiden Netzen benutzten Komponenten gehören z. B. HTML und HTTP.

IPSec. Ein von der IETF entwickelter IPS-Standard (IPS = Internet Protocol Security). IPSec ist ein Protokoll der Vermittlungsschicht, das entwickelt wurde, um Services für die Gewährleistung der Sicherheit bei der Verschlüsselung zur Verfügung zu stellen, die kombinierte Funktionen zur Authentifizierung, Sicherung der Integrität, Zugriffssteuerung und Wahrung der Vertraulichkeit flexibel unterstützen. Aufgrund seiner leistungsfähigen Funktionen bei der Authentifizierung wurde dieser Standard von vielen Lieferanten von VPN-Produkten als Protokoll zum Aufbau sicherer Punkt-zu-Punkt-Verbindungen im Internet übernommen.

ISO. International Standards Organization.

ITU. International Telecommunication Union.

J

Java. Von Sun Microsystems, Incorporated, entwickelte plattformunabhängige Computertechnologien, die für den Netzbetrieb optimiert sind. Die Java-Umgebung besteht aus dem Java-Betriebssystem (Java-OS), den virtuellen Maschinen für verschiedene Plattformen, der

objektorientierten Java-Programmiersprache und einer Reihe von Klassenbibliotheken.

Java Virtual Machine (JVM). Der Teil der Java-Laufzeitumgebung, der zum Interpretieren von Bytecodes eingesetzt wird.

Java-Anwendung. Ein eigenständiges Programm, das in der Programmiersprache Java geschrieben ist. Es wird außerhalb eines Web-Browsers ausgeführt.

Java-Applet. *Siehe* Applet. *Gegensatz zu* Java-Anwendung.

Java-Klasse. Eine Einheit mit Java-Programmcode.

Java-Sprache. Eine von Sun Microsystems entwickelte Programmiersprache, die speziell für die Verwendung in Applet- und Agent-Anwendungen konzipiert wurde.

K

KeyStore (Schlüsselspeicher). Eine DL zum Speichern von Identitätsnachweisen für Trust Authority-Komponenten, z. B. Schlüssel und Zertifikate, in einem verschlüsselten Format.

Klartext. Nicht verschlüsselte Daten. *Synonym zu* unverschlüsselter Text.

Klasse. Beim objektorientierten Entwurf bzw. bei der objektorientierten Programmierung eine Gruppe von Objekten, die über eine gemeinsame Definition verfügen und aus diesem Grund mit denselben Merkmalen, Verarbeitungsoperationen und Funktionsweisen arbeiten.

Kryptographie. Bei der Sicherung von Computern die Prinzipien, Verfahren und Methoden zur Verschlüsselung von unverschlüsseltem und zur Entschlüsselung von verschlüsseltem Text.

L

LDAP. Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP). Ein Protokoll, mit dem auf das Directory zugegriffen werden kann.

Liste der ausgestellten Zertifikate (ICL). Eine vollständige Liste der ausgestellten Zertifikate sowie deren aktueller Status. Die Zertifikate sind anhand der Seriennummer und des Status indexiert. Diese Liste wird vom CA verwaltet und in der CA-Datenbank gespeichert.

M

MAC. Message Authentication Code - Nachrichtenauthentifizierungscode.

MD2. Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Sie wird zusammen mit MD5 in den PEM-Protokollen verwendet.

MD4. Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Ihre Geschwindigkeit übersteigt die von MD2 um ein Mehrfaches.

MD5. Eine unidirektionale Nachrichtenauszugs-Hash-Funktion, die von Ron Rivest entwickelt wurde. Sie stellt eine verbesserte Version von MD4 dar. MD5 verarbeitet Eingabetext in 512-Bit-Blöcken, die in 16 32-Bit-Unterblöcke aufgeteilt werden. Die Ausgabe des Algorithmus ist eine Gruppe von vier 32-Bit-Blöcken, die verkettet werden und so einen 128-Bit-Hash-Wert bilden. Diese Funktion wird ebenfalls zusammen mit MD2 in dem PEM-Protokollen verwendet.

Modulus. In dem auf öffentlichen Schlüsseln basierenden RSA-Verschlüsselungssystem das Produkt (`n`) aus zwei hohen Primzahlen: `p` und `q`. Die optimale Größe für einen RSA-Modulus hängt von den individuellen Sicherheitsanforderungen ab. Je größer der Modulus, desto höher die Sicherheit. Die momentan von den RSA Laboratories empfohlenen Schlüsselgrößen hängen vom geplanten Einsatz des Schlüssels ab. Hierbei werden 768 Bit für Schlüssel zum persönlichen Gebrauch, 1024 Bit für den Unternehmensbereich und 2048 Bit für extrem wertvolle Schlüssel wie z. B. CA-Schlüsselpaare angegeben. Ein 768-Bit-Schlüssel wird voraussichtlich bis mindestens zum Jahr 2004 sicher sein.

Multipurpose Internet Mail Extensions (MIME). Eine frei verfügbare Gruppe von Spezifikationen, die den Austausch von Text in Sprachen mit unterschiedlichen Zeichensätzen ermöglicht. Diese Spezifikationen unterstützen auch den Austausch von Multimedia-E-Mail zwischen unterschiedlichen Computersystemen, die Internet-Mail-Standards verwenden. So können E-Mail-Nachrichten beispielsweise andere Zeichensätze als den US-ASCII-Satz sowie erweiterten Text, Bilder oder Tondaten enthalten.

N

Nachrichtenauszug. Eine irreversible Funktion, bei der auf der Basis einer Nachricht beliebiger Länge eine Datenmenge mit fester Länge generiert wird. Bei MD5 handelt es sich z. B. um einen Nachrichtenauszugsalgorithmus.

Nachrichtenauthentifizierungscode (MAC). Ein geheimer Schlüssel, der von Sender und Empfänger gemeinsam benutzt wird. Der Sender authentifiziert sich und der Empfänger prüft die hierbei zur Verfügung gestellten Daten. Bei Trust Authority werden MAC-Schlüssel für CA- und Prüfkomponenten in den KeyStores gespeichert.

National Security Agency (NSA). Die offizielle Sicherheitsbehörde der US-Regierung.

NIST. National Institute of Standards and Technology, früher NBS (National Bureau of Standards). Aufgabe dieses Instituts ist die Unterstützung offener Standards und der Interoperabilität in den verschiedenen Bereichen der Computerbranche.

NLS. National Language Support - Unterstützung in der Landessprache.

NSA. National Security Agency.

O

Objekt. Beim objektorientierten Design oder bei der objektorientierten Programmierung eine abstrakte Entität, die zur Abgrenzung bestimmter Daten und der zugehörigen Operationen dient. *Siehe auch* Klasse.

Objekt-ID (OID). Ein von einer Verwaltungsfunktion zugeordneter Datenwert, der den in ASN.1 definierten Typ aufweist.

Objektart. Die Art von Objekt, die im Directory gespeichert werden kann. Beispiele sind eine Firma, ein Konferenzraum, eine Einheit, eine Person, ein Programm oder ein Prozeß.

ODBC. Open Database Connectivity.

Öffentlicher Schlüssel. In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel anderen Benutzern zur Verfügung. Er ermöglicht diesen Benutzern die Weiterleitung einer Transaktion an den Eigner des Schlüssels sowie die Prüfung einer digitalen Unterschrift. Mit einem öffentlichen Schlüssel verschlüsselte Daten können nur mit dem entsprechenden privaten Schlüssel entschlüsselt werden. *Gegensatz zu* Privater Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.

Open Database Connectivity (ODBC). Ein Standard für den Zugriff auf unterschiedliche Datenbanksysteme.

Open Systems Interconnect (OSI). Der Name der von ISO genehmigten Computernetzstandards.

OSI. Open Systems Interconnect.

P

PC-Karte. Eine mit einer Smart-Card vergleichbare Einheit, die auch als PCMCIA-Karte bezeichnet wird. Sie ist etwas größer als eine Smart-Card und verfügt im allgemeinen über eine höhere Kapazität.

PEM. Privacy-Enhanced Mail.

PKCS. Public Key Cryptography Standards.

PKCS #1. *Siehe* Public Key Cryptography Standards.

PKCS #10. *Siehe* Public Key Cryptography Standards.

PKCS #11. *Siehe* Public Key Cryptography Standards.

PKCS #12. *Siehe* Public Key Cryptography Standards.

PKCS #7. *Siehe* Public Key Cryptography Standards.

PKI. Public Key Infrastructure.

PKIX. PKI auf X.509v3-Basis.

PKIX Certificate Management Protocol (PKIX CMP). Ein Protokoll, das Verbindungen mit PKIX-kompatiblen Anwendungen ermöglicht. PKIX CMP verwendet als primäres Transportverfahren TCP/IP, es ist jedoch eine Abstraktionsebene oberhalb der Sockets-Schicht vorhanden. Hierdurch können zusätzliche Datenübertragungsoperationen mit Sendeaufrufen (Polling) unterstützt werden.

PKIX CMP. PKIX Certificate Management Protocol.

PKIX-Empfangseinheit. Der öffentliche HTTP-Server, der von einer bestimmten Registrierungsdomäne verwendet wird, um Anforderungen der Client-Anwendung von Trust Authority zu empfangen.

Privacy-Enhanced Mail (PEM). Der vom Internet Architect Board (IAB) genehmigte Internet-Standard für die verbesserte Wahrung der Vertraulichkeit, der die sichere Übertragung elektronischer Post (E-Mail) über das Internet ermöglicht. Die PEM-Protokolle regeln Verschlüsselung, Authentifizierung, Nachrichtenintegrität und Schlüsselverwaltung.

Privater Schlüssel. In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel nur für seinen Eigner zur Verfügung. Er ermöglicht dem Eigner das Empfangen einer privaten Transaktion oder eine digitale Unterschrift. Die mit einem privaten Schlüssel unterzeichneten Daten können nur mit dem entsprechenden öffentlichen Schlüssel geprüft werden. *Gegensatz zu* Öffentlicher Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.

Protokoll. Eine vereinbarte Konvention für die Kommunikation zwischen Computern.

Protokollierungssubsystem. Bei Trust Authority ein Subsystem, das die Unterstützungsfunktionen zum Protokollieren von sicherheitsrelevanten Aktionen bereitstellt. Es entspricht den Empfehlungen, die im X9.57-Standard unter *Public Key Cryptography for the Financial Services Industry* definiert wurden.

Proxy-Server. Eine Einheit, die zwischen einem Computer, der eine Zugriffsanforderung absetzt (Computer A) und einem Computer, auf den zugegriffen werden soll (Computer B), implementiert ist. Wenn ein Endbenutzer eine Anforderung für eine Ressource über Computer A absetzt, wird diese an den Proxy-Server gelei-

tet. Dieser sendet die Anforderung an Computer B, erhält von diesem die Antwort und leitet diese an den Endbenutzer weiter. Mit Hilfe eines Proxy-Servers kann über einen Computer, der sich innerhalb einer Firewall befindet, auf das World Wide Web zugegriffen werden.

Prüf-Client. Jeder Client im System, der Prüfereignisse an den Trust Authority-Prüf-Server sendet. Bevor ein Prüf-Client ein Ereignis an den Prüf-Server sendet, stellt er eine Verbindung zu diesem her. Nach der Herstellung der Verbindung verwendet der Client die Client-Bibliothek des Prüfsubsystems, um Ereignisse an den Prüf-Server zu übertragen.

Prüf-Server. Ein Trust Authority-Server, der zum Empfangen von Prüfereignissen von Prüf-Clients und zum Aufzeichnen dieser Ereignis in einem Prüfprotokoll dient.

Prüfprotokoll. Daten in Form eines logischen Pfades, die eine Folge von Ereignissen verbinden. Mit dem Prüfprotokoll können Transaktionen oder der bisherige Verlauf einer bestimmten Aktivität verfolgt werden.

Prüfprotokoll. Bei Trust Authority eine Tabelle in einer Datenbank, in der für jedes Prüfereignis ein Datensatz gespeichert wird.

Prüfzeichenfolge. Eine Zeichenfolge, die von einem Server oder einer Anwendung gesendet wird und zum Anfordern der Benutzerberechtigung dient. Der Benutzer, der zur Authentifizierung aufgefordert wird, unterzeichnet die Prüfzeichenfolge mit einem privaten Schlüssel. Der öffentliche Schlüssel des Benutzers sowie die unterzeichnete Prüfzeichenfolge werden zurück an den Server oder die Anwendung gesendet, der bzw. die die Authentifizierung anforderte. Der Server versucht anschließend, die unterzeichnete Prüfzeichenfolge mit Hilfe des öffentlichen Schlüssels des Benutzers zu entschlüsseln. Wenn die entschlüsselte Prüfzeichenfolge mit der ursprünglich gesendeten Prüfzeichenfolge übereinstimmt, gilt der Benutzer als authentifiziert.

Public Key Cryptography Standards (PKCS). Informelle, herstellerübergreifende Standards, die im Jahr 1991 von den RSA Laboratories in Zusammenarbeit mit Repräsentanten verschiedener Computerhersteller entwickelt wurden. Diese Standards umfassen die RSA-Verschlüsselung, die Diffie-Hellman-Vereinbarung, die kennwortbasierte Verschlüsselung sowie die Syntax für erweiterte Zertifikate, verschlüsselte Nachrichten, Daten zu privaten Schlüsseln und für die Zertifizierung.

- PKCS #1 beschreibt ein Verfahren zum Verschlüsseln von Daten mit Hilfe des RSA-Verschlüsselungssystems auf der Basis öffentlicher Schlüssel. Er dient zur Erstellung digitaler Unterschriften und Briefumschläge.
- PKCS #7 definiert ein allgemeines Format für verschlüsselte Nachrichten.
- PKCS #10 definiert eine Standardsyntax für Zertifizierungsanforderungen.
- PKCS #11 definiert eine Programmierschnittstelle für Verschlüsselungseinheiten, z. B. Smart-Cards, die unabhängig vom verwendeten technologischen Konzept ist.
- PKCS #12 definiert ein portierbares Format zum Speichern oder Transportieren der privaten Schlüssel, Zertifikate und sonstiger geheimer Daten etc. eines Benutzers.

Public Key Infrastructure (PKI). Ein Standard für Sicherheitssoftware, der auf der Verschlüsselung mit Hilfe öffentlicher Schlüssel basiert. Bei PKI handelt es sich um ein System digitaler Zertifikate, Zertifikatsaussteller, Registrierungsstellen, Zertifikatverwaltungsservices und verteilter Verzeichnisservices. Er dient zum Prüfen der Identität und Berechtigung aller Parteien, die an Transaktionen beteiligt sind, die über das Internet ausgeführt werden. Diese Transaktionen umfassen möglicherweise Operationen, zu deren Ausführung eine Identitätsprüfung erforderlich ist. Sie dienen z. B. zur Bestätigung des Ursprungs von Senderechtanforderungen, E-Mail-Nachrichten oder Finanztransaktionen.

PKI erreicht dieses Ziel dadurch, daß öffentliche Chiffrierschlüssel und Benutzerzertifikate für die Authentifizierung durch eine berechtigte Einzelperson oder ein berechtigtes Unternehmen verfügbar gemacht werden. Er stellt Online-Verzeichnisse bereit, die die öffentlichen Chiffrierschlüssel und Zertifikate enthalten, die zur Überprüfung der digitalen Zertifikate, Identitätsnachweise sowie der digitalen Unterschriften verwendet werden.

PKI stellt außerdem Funktionen zur schnellen und effizienten Antwort auf Prüfabfragen und Anforderungen für öffentliche Chiffrierschlüssel bereit. Der Standard dient darüber hinaus zur Identifizierung potentieller Sicherheitslücken im System und zur Verwaltung von Ressourcen zur Bearbeitung von Sicherheitsverletzungen. PKI bietet außerdem einen digitalen Zeitmarkenservice für wichtige Unternehmenstransaktionen.

R

RA. Registration Authority - Registrierungsstelle.

RA Desktop. Ein Java-Applet, das den RAs eine Grafikschnittstelle für die Verarbeitung von Anforderungen für Identitätsnachweise und zur Verwaltung dieser Nachweise während ihrer Gültigkeitsdauer zur Verfügung stellt.

RA-Server. Der Server für die RA-Komponente von Trust Authority.

RC2. Eine variable Schlüsselgrößen-Block-Cipher, die von Ron Rivest für RSA Data Security entwickelt wurde. *RC* steht für *Ron's Code* oder *Rivest's Cipher*. Sie arbeitet schneller als DES und löst diese Block-Cipher ab. Durch die Verwendung geeigneter Schlüsselgrößen

kann sie in Bezug auf eine ausgedehnte Schlüsselsuche flexibler als DES gestaltet werden. Sie verfügt über eine Blockgröße von 64 Bit und arbeitet auf Softwareebene zwei- bis dreimal schneller als DES. RC2 kann in denselben Modi eingesetzt werden wie DES.

Durch eine Vereinbarung zwischen SPA (Software Publishers Association) und der US-Regierung nimmt RC2 einen speziellen Status ein. Hierdurch ist das Genehmigungsverfahren für den Export einfacher und schneller, als dies bei anderen Verschlüsselungsprodukten der Fall ist. Um die Voraussetzungen für eine rasche Exportgenehmigung zu erfüllen, muß ein Produkt mit einigen Ausnahmen die RC2-Schlüsselgröße auf 40 Bit beschränken. Eine zusätzliche Zeichenfolge kann verwendet werden, um Nichtberechtigte abzuwehren, die versuchen, eine umfangreiche Tabelle möglicher Verschlüsselungsvarianten vorauszuberechnen.

Regel-Exit. In einer Registrierungsfunktion ein auf Unternehmensebene definiertes Programm, das von der Registrierungsanwendung aufgerufen wird. Die Regeln eines Regel-Exits implementieren die Unternehmens- und Sicherheitsbenutzervorgaben eines Unternehmens für den Registrierungsprozeß.

Registrator. Ein Benutzer, der für den Zugriff auf RA Desktop sowie zur Verwaltung und Anforderung von Zertifikaten berechtigt ist.

Registrierter Name (DN). Der eindeutige Name eines im Directory gespeicherten Dateneintrags. Der DN dient zur eindeutigen Identifizierung der Position eines Eintrags in der hierarchischen Struktur des Directory.

Registrierung. Bei Trust Authority das Abrufen von Identitätsnachweisen für die Verwendung über das Internet. Bei der Registrierung werden Zertifikate angefordert, erneuert und widerrufen.

Registrierungsattribut. Eine Registrierungsvariable, die in einem Registrierungsformular enthalten ist. Ihr Wert gibt die Informationen wider, die während der Registrierung erfaßt werden. Der Wert des Registrierungsattributs bleibt während der gesamten Gültigkeitsdauer des Identitätsnachweises gleich.

Registrierungsdatenbank. Diese Datenbank enthält Informationen zu Zertifikatsanforderungen und ausgestellten Zertifikaten. In der Datenbank werden Registrierungsdaten gespeichert und alle Änderungen aufgezeichnet, die während der Gültigkeitsdauer an einem Zertifikat vorgenommen werden. Die Datenbank kann durch RA-Prozesse und Regel-Exits oder durch den Registrator aktualisiert werden.

Registrierungsdomäne. Eine Gruppe von Ressourcen, Regeln und Konfigurationsoptionen, die sich auf bestimmte Registrierungsprozesse für Zertifikate beziehen. Der Domänenname stellt einen untergeordneten Wert zur URL-Adresse dar, die zur Ausführung der Registrierungsfunktion eingesetzt wird.

Registrierungsfunktion. Ein Trust Authority-Anwendungsgerüst, das spezielle Verfahren zur Registrierung von Entitäten (z. B. Browser, Router, E-Mail-Einheiten und sichere Client-Anwendungen) und zur Verwaltung von Zertifikaten während ihrer Gültigkeitsdauer bereitstellt.

Registrierungsprozeß. Bei Trust Authority die Schritte, die zur Überprüfung eines Benutzers ausgeführt werden. Durch den Registrierungsprozeß werden Benutzer sowie deren öffentliche Schlüssel zertifiziert, um sie zur Teilnahme an den gewünschten Transaktionen zu berechtigen. Er kann lokal oder Web-gestützt, automatisch oder von einer tatsächlich mit Personen besetzten Registrierungsstelle ausgeführt werden.

Registrierungsstelle (RA). Die Software, die zur Verwaltung digitaler Zertifikate verwendet wird und sicherstellt, daß die Unternehmensregeln vom ersten Empfang einer Registrierungsanforderung bis zum Zertifikatswiderruf angewendet werden.

Registrierungsvariable. *Siehe* Registrierungsattribut.

RSA. Ein auf öffentlichen Schlüsseln basierender Verschlüsselungsalgorithmus, der nach seinen Erfindern (Rivest, Shamir und Adelman) benannt wurde. Er wird zur Verschlüsselung und für digitale Unterschriften verwendet.

S

S/MIME. Ein Standard, der das Unterzeichnen und Verschlüsseln von elektronischer Post (E-Mail) unterstützt, die über das Internet übertragen wird. *Siehe* MIME.

Schema. Beim Directory die interne Struktur, die zur Definition der Beziehungen zwischen den verschiedenen Objektarten verwendet wird.

Schlüssel. Bei der Verschlüsselung ein Wert, der zum Ver- und Entschlüsseln von Informationen verwendet wird.

Schlüsselpaar. Zusammengehörende Schlüssel, die bei der asymmetrischen Verschlüsselung eingesetzt werden. Ein Schlüssel wird zur Verschlüsselung, der andere zur Entschlüsselung verwendet.

Schlüsselpaar aus öffentlichem und privatem Schlüssel. Ein Schlüsselpaar aus öffentlichem und privatem Schlüssel stellt ein grundlegendes Element der Verschlüsselung auf der Basis von Schlüsselpaaren dar. (Diese Form der Verschlüsselung wurde im Jahr 1976 von Whitfield Diffie und Martin Hellman eingeführt, um Probleme bei der Schlüsselverwaltung zu lösen.) Nach diesem Konzept erhält jeder Benutzer ein Schlüsselpaar, bei dem einer als öffentlicher und einer als privater Schlüssel bezeichnet wird. Der öffentliche Schlüssel ist hierbei allgemein bekannt, der private Schlüssel wird hingegen geheimgehalten. Sender und

Empfänger müssen geheime Daten nicht gemeinsam benutzen. Alle Kommunikationsoperationen werden lediglich auf der Basis öffentlicher Schlüssel ausgeführt. Die privaten Schlüssel werden niemals übertragen oder gemeinsam verwendet. Auf diese Weise ist es nicht mehr notwendig, sich auf die Sicherheit eines Übertragungskanals gegenüber Manipulationen zu verlassen. Die einzige Anforderung ist, daß öffentliche Schlüssel den entsprechenden Benutzern in einer gesicherten (authentifizierten) Weise (z. B. in einem gesicherten Verzeichnis) zugeordnet werden. Jeder Benutzer kann nun mit Hilfe dieser öffentlichen Daten eine vertrauliche Nachricht senden. Diese Nachricht kann nur mit einem privaten Schlüssel entschlüsselt werden, auf den allein der gewünschte Empfänger zugreifen kann. Darüber hinaus kann die Verschlüsselung auf der Basis von Schlüsselpaaren nicht nur zur Gewährleistung der Vertraulichkeit (Verschlüsselung), sondern auch für die Authentifizierung (digitale Unterschriften) eingesetzt werden.

Secure Electronic Transaction (SET). Ein Branchenstandard für die Durchführung sicherer Kredit- oder Kundenkartenzahlungen über nicht gesicherte Netze. Der Standard formuliert Definitionen für die Authentifizierung von Kartenhaltern, Händlern sowie der Banken, durch die die Karten ausgestellt werden, da er die Ausstellung von Zertifikaten anfordert.

Secure Sockets Layer (SSL). Ein IETF-Standardübertragungsprotokoll mit integrierten Sicherheitsservices, die für den Endbenutzer möglichst transparent sind. Es stellt einen digitalen, sicheren Kommunikationskanal zur Verfügung.

Ein SSL-fähiger Server empfängt SSL-Verbindungsanforderungen im allgemeinen an einem anderen Anschluß (Port) als normale HTTP-Anforderungen. SSL erstellt eine Sitzung, in der die Austauschsignale zum Herstellen der Kommunikation zwischen zwei Modems nur einmal gesendet werden müssen. Anschließend wird die Kommunikation verschlüsselt und die Nachrichtenintegrität wird solange überprüft, bis die SSL-Sitzung abgelaufen ist.

Server. (1) In einem Netz eine Datenstation, die anderen Stationen Funktionen zur Verfügung stellt, wie beispielsweise ein Datei-Server. (2) In TCP/IP ein System in einem Netz, das die Anforderungen eines Systems an einem anderen Standort verarbeitet. Dieses Konzept wird als Client/Server-Modell bezeichnet.

Server-Zertifikat. Ein digitales Zertifikat, das von einem CA ausgegeben wird und es einem Web-Server ermöglicht, SSL-gestützte Transaktionen auszuführen. Wenn ein Browser über das SSL-Protokoll eine Verbindung zum Server herstellt, sendet der Server seinen öffentlichen Schlüssel an den Browser. Hierdurch kann die Identität des Servers authentifiziert werden und es können verschlüsselte Daten an den Server gesendet werden. *Siehe auch* CA-Zertifikat, Digitales Zertifikat, *und* Browser-Zertifikat.

Servlet. Ein Server-Programm, das zusätzliche Funktionen für Server zur Verfügung stellt, die Java unterstützen.

SET. Secure Electronic Transaction.

SGML. Standard Generalized Markup Language.

SHA-1 (Secure Hash Algorithm). Ein von NIST und NSA entwickelter Algorithmus, der beim DSS (Digital Signature Standard) verwendet wird. Der Standard wird als Secure Hash Standard bezeichnet; SHA ist der Algorithmus, der von diesem Standard verwendet wird. Er generiert einen 160-Bit-Hash-Code.

Sicherheitsdomäne. Eine Gruppe (z. B. Unternehmen, Arbeitsgruppe, Projektteam), deren Zertifikate vom gleichen CA zertifiziert wurden. Benutzer, die über ein von einem CA unterzeichnetes Zertifikat verfügen, können der Identität eines anderen Benutzers vertrauen, der ein Zertifikat besitzt, das vom selben CA unterzeichnet worden ist.

Sicherungsmodell. Eine Organisationskonvention, die regelt, wie Zertifikatsaussteller (CAs) andere Zertifikatsaussteller zertifizieren können.

Simple Mail Transfer Protocol (SMTP). Ein Protokoll, mit dem elektronische Post über das Internet übertragen wird.

Site-Zertifikat. Dieser Zertifikatstyp ist mit einem CA-Zertifikat vergleichbar, gilt jedoch nur für eine bestimmte Website. *Siehe auch* CA-Zertifikat.

Smart-Card. Eine Hardwarekomponente, normalerweise in der Größe einer Kreditkarte, auf der die digitalen Schlüssel eines Benutzers gespeichert werden können. Eine Smart-Card kann kennwortgeschützt werden.

SMTP. Simple Mail Transfer Protocol.

SSL. Secure Sockets Layer.

Standard Generalized Markup Language (SGML). Ein Standard zur Beschreibung von Formatierungssprachen. HTML basiert auf SGML.

Symmetrische Verschlüsselung. Eine Form der Verschlüsselung, bei der sowohl für die Ver- als auch für die Entschlüsselung derselbe Schlüssel verwendet wird. Die Sicherheit dieses Verfahren basiert auf dem Schlüssel. Wird dieser öffentlich bekanntgegeben, können die mit ihm bearbeiteten Nachrichten von jedem Benutzer ver- und entschlüsselt werden. Der Inhalt der übertragenen Daten kann nur dann geheimgehalten werden, wenn der Schlüssel nur den jeweils berechtigten Personen bekannt ist. *Gegensatz zu* Asymmetrische Verschlüsselung.

Symmetrischer Schlüssel. Ein Schlüssel, der sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet werden kann. *Siehe auch* Symmetrische Verschlüsselung.

T

TCP/IP. Transmission Control Protocol/Internet Protocol.

TP. Trust Policy = Sicherungsregel.

Transaktions-ID. Eine Kennung, die die RA als Antwort auf eine Anforderung für eine Vorabregistrierung zur Verfügung stellt. Mit dieser ID kann ein Benutzer, der die Client-Anwendung von Trust Authority ausführt, ein vorab genehmigtes Zertifikat erhalten.

Transmission Control Protocol/Internet Protocol (TCP/IP). Eine Gruppe von Übertragungsprotokollen, die Peer-zu-Peer-Konnektivitätsfunktionen für lokale Netze (LANs) und Weitverkehrsnetze (WANs) unterstützen.

Triple DES. Ein symmetrischer Algorithmus, bei dem der unverschlüsselte Text dreimal verschlüsselt wird. Obwohl für diese Mehrfachverschlüsselung zahlreiche Methoden existieren, stellt die Triple DES-Verschlüsselung, die auf drei verschiedenen Schlüsseln basiert, das sicherste dieser Verfahren dar.

Trust Authority. Eine integrierte IBM SecureWay-Sicherheitslösung, die die Ausstellung, Erneuerung und den Widerruf digitaler Zertifikate unterstützt. Diese Zertifikate können für eine breite Palette von Internet-Anwendungen eingesetzt werden und bieten eine Möglichkeit zur Authentifizierung von Benutzern und zur Gewährleistung einer gesicherten Kommunikation.

Tunnel. In der VPN-Technologie eine virtuelle Punkt-zu-Punkt-Verbindung, die auf Anfrage über das Internet hergestellt wird. Während der Verbindung können ferne Benutzer den Tunnel verwenden, um sichere, verschlüsselte und gekapselte Informationen mit Servern im privaten Netz eines Unternehmens auszutauschen.

U

Unbestreitbarkeit. Die Verwendung eines digitalen, privaten Schlüssels, um zu verhindern, daß der Unterzeichner eines Dokuments dessen Unterzeichnung leugnet.

Unicode. Ein 16-Bit-Zeichensatz, der in ISO 10646 definiert ist. Der Unicodestandard für die Verschlüsselung von Zeichen ist ein internationaler Zeichencode für die Informationsverarbeitung. Er umfaßt die grundlegenden, weltweit verwendeten Prozeduren und bildet die Basis für die Internationalisierung und Lokalisierung von Software. Der gesamte Quellencode in der Java-Programmierungsumgebung wird in Unicode geschrieben.

Unternehmensprozeßobjekte. Eine Codegruppe, die zur Ausführung einer bestimmten Registrierungsoperation, z. B. zum Prüfen des Registrierungsstatus oder zur Bestätigung des Sendens eines öffentlichen Schlüssels, verwendet wird.

Unternehmensprozeßschablone. Eine Gruppe von Unternehmensprozeßobjekten, die in einer bestimmten Reihenfolge ausgeführt werden.

Unterstützung in der Landessprache (NLS). Unterstützung für unterschiedliche länderspezifische Angaben in einem Produkt. Hierzu gehören die Sprache, die Währung, das Datums- und Zeitformat und die Darstellung von Zahlen.

Unterzeichnen. Die Verwendung eines digitalen privaten Schlüssels zum Generieren einer Unterschrift. Diese Unterschrift dient dazu, zu beweisen, daß ein bestimmter Benutzer für die von ihm unterzeichnete Nachricht verantwortlich ist und diese akzeptiert.

Unterzeichnen/Prüfen. Als Unterzeichnen wird die Verwendung eines privaten Schlüssels zum Generieren einer Unterschrift bezeichnet. Unter Prüfen versteht man die Verwendung des entsprechenden öffentlichen Schlüssels zur Verifizierung dieser Unterschrift.

Unverschlüsselter Text. Nicht verschlüsselte Daten. *Synonym zu* Klartext.

URL. Uniform Resource Locator - URL-Adresse.

URL-Adresse. Ein Schema für die Adressierung von Ressourcen im Internet. Die URL-Adresse gibt das verwendete Protokoll sowie den Host-Namen und die IP-Adresse an. Außerdem enthält er Angaben zur Anschlußnummer, zum Pfad sowie weitere Ressourcendetails, die erforderlich sind, um über eine bestimmte Maschine auf eine Ressource zuzugreifen.

UTF-8. Ein Umsetzungsformat. Es ermöglicht Informationsverarbeitungssystemen, die nur die Verarbeitung von 8-Bit-Zeichensätzen unterstützen, die Umsetzung von 16-Bit-Unicode in ein 8-Bit-Äquivalent und umgekehrt, ohne daß hierbei Informationen verlorengehen.

V

Verkettungsprüfung. Die Gültigkeitsprüfung aller CA-Unterschriften in der Trust-Hierarchie, über die ein bestimmtes Zertifikat ausgestellt wurde. Wenn z. B. das Unterschriftszertifikat eines CA über einen anderen CA ausgestellt wurde, werden bei der Gültigkeitsprüfung des vom Benutzer vorgelegten Zertifikats beide Unterschriften geprüft.

Verschlüsseln. Das Umordnen von Informationen, so daß nur Personen, die über den richtigen Entschlüsselungscode verfügen, die ursprünglichen Informationen durch Entschlüsselung abrufen können.

Verschlüsselt. Die Eigenschaft von Daten, die nach einem bestimmten System umgesetzt wurden, um deren Bedeutung unkenntlich zu machen.

Verschlüsselung/Entschlüsselung. Die Verwendung des öffentlichen Schlüssels des gewünschten Empfängers zum Verschlüsseln von Daten für diese Person. Der Empfänger verwendet anschließend den privaten Schlüssel seines Schlüsselpaares, um die Daten zu entschlüsseln.

Vertrauensdomäne. Eine Gruppe von Entitäten, deren Zertifikate vom gleichen CA zertifiziert wurden.

Vertraulichkeit. Die Wahrung der Geheimhaltung bestimmter Informationen gegenüber nicht berechtigten Personen.

Vertraulichkeit. Der Schutz von Daten gegen den Zugriff nicht berechtigter Personen.

Virtual Private Network (VPN). Ein privates Datennetz, das ferne Verbindungen nicht über Telefonleitungen, sondern über das Internet herstellt. Da der Zugriff der Benutzer auf die Netzressourcen eines Unternehmens nicht über eine Telefongesellschaft, sondern über einen Internet Service Provider (ISP) erfolgt, können diese durch den Einsatz von VPN deutliche Einsparungen bei Fernzugriffen erzielen. Ein VPN erhöht auch die Sicherheit beim Datenaustausch. Bei der herkömmlichen Firewall-Technologie kann zwar der Inhalt der Nachricht verschlüsselt werden, nicht jedoch die Quellen- und Zieladressen. Bei der VPN-Technologie können die Benutzer eine Tunnelverbindung herstellen, bei der das gesamte Datenpaket (Header- und Datenkomponente) verschlüsselt und gekapselt ist.

Vorabregistrierung. Bei Trust Authority ein Prozeß, mit dem ein bestimmter Benutzer (normalerweise ein Administrator) andere Benutzer registrieren kann. Wenn die Anforderung genehmigt wird, stellt die RA Informationen zur Verfügung, mit denen der Benutzer später mit Hilfe der Client-Anwendung von Trust Authority ein Zertifikat erhalten kann.

VPN. Virtual Private Network.

W

Web-Browser. Auf einem PC ausgeführte Client-Software, mit der ein Benutzer im World Wide Web navigieren oder lokale HTML-Seiten anzeigen kann. Der Web-Browser ist ein Abfrage-Tool, das universellen Zugriff auf die umfangreichen Hypermedia-Datensammlungen ermöglicht, die im Web und im Internet zur Verfügung gestellt werden. Manche Browser können Text und Grafik anzeigen, während andere Browser auf die Textanzeige beschränkt sind. Die meisten Browser unterstützen die Hauptformen der Internet-Kommunikation, z. B. die Ausführung von FTP-Transaktionen.

Web-Server. Ein Server-Programm, das auf Anforderungen von Browser-Programmen nach Informationsressourcen antwortet. *Siehe auch* Server.

WebSphere Application Server. Ein IBM Produkt, das Benutzer bei der Entwicklung und Verwaltung von Websites mit einem hohen Leistungsumfang unterstützt. Es erleichtert den Übergang vom einfachen Web Publishing zu komplexen e-business-Anwendungen im Web. Der WebSphere Application Server besteht aus einer Java-Servlet-Maschine, die unabhängig vom Web-Server und dem verwendeten Betriebssystem arbeitet.

World Wide Web (WWW). Der Teil des Internets, in dem ein Netz von Verbindungen zwischen Computern aufgebaut wird, auf denen Hypermediamaterial gespeichert ist. Dieses Material stellt neben Informationen auch Verbindungen (Hyperlinks) zu anderem Material im World Wide Web und Internet zur Verfügung. Der Zugriff auf WWW-Ressourcen erfolgt über einen Web-Browser.

X

X.500. Ein Standard für die Implementierung eines multifunktionalen, verteilten und vervielfältigten Verzeichnisservices durch die Verbindung von Computersystemen. Dieser Standard wurde gemeinsam definiert von der bisher als CCITT bekannten International Telecommunications Union (ITU) sowie der International Organization for Standardization und der International Electro-Chemical Commission (ISO/IEC).

X.509 Version 3-Zertifikat. Das X.509v3-Zertifikat verfügt über erweiterte Datenstrukturen für die Speicherung und das Abrufen von Informationen zu Zertifikatsanträgen, zur Zertifikatsverteilung und zu Zertifikatswiderrufen sowie zu Sicherheitsregeln und digitalen Unterschriften.

X.509v3-Prozesse dienen zum Erstellen von CRLs mit Zeitmarken für alle Zertifikate. Bei jeder Verwendung eines Zertifikats ermöglichen die X.509v3-Funktionen der Anwendung, die Gültigkeit des Zertifikats zu überprüfen. Die Anwendung kann außerdem feststellen, ob sich das Zertifikat auf der Zertifikatswiderrufsliste (CRL) befindet. CRLs unter X.509v3 können für eine bestimmte Gültigkeitsperiode erstellt werden. Sie können auch auf anderen Kriterien basieren, die zur Aufhebung der Gültigkeit eines Zertifikats führen. Wenn z. B. ein Mitarbeiter ein Unternehmen verläßt, wird sein Zertifikat in der CRL eingetragen.

X.509-Zertifikat. Ein weitverbreiteter Zertifikatsstandard, der entwickelt wurde, um die sichere Verwaltung und Verteilung von digital unterzeichneten Zertifikaten

über sichere Internet-Netze zu unterstützen. Das X.509-Zertifikat definiert Datenstrukturen, die Prozeduren für die Verteilung öffentlicher Schlüssel unterstützen, die von zuverlässigen Stellen digital unterzeichnet sind.

Z

Zertifikatsaussteller (CA). Die Software, die zur Einhaltung der Sicherheitsregeln eines Unternehmens und zur Vergabe gesicherter elektronischer Identitäten in Form von Zertifikaten dient. Der CA verarbeitet die Anforderungen von RAs zum Ausstellen, Erneuern und Widerrufen von Zertifikaten. Er kooperiert mit der RA, um Zertifikate und CRLs im Directory zu veröffentlichen. *Siehe auch* Digitales Zertifikat.

Zertifikatserweiterung. Eine Zusatzfunktion des X.509v3-Zertifikatformats, die zur Einbindung zusätzlicher Felder in das Zertifikat dient. Es stehen Standard- und benutzerdefinierte Erweiterungen zur Verfügung. Die Standarderweiterungen dienen verschiedenen Zwecken und umfassen Schlüssel- und Regelinformationen, Betreff- und Ausstellerattribute sowie Einschränkungen, die für den Zertifizierungspfad gelten.

Zertifikatsprofil. Eine Gruppe von Kenndaten, die den gewünschten Zertifikatstyp definieren (z. B. SSL- oder IPSec-Zertifikate). Das Profil vereinfacht die Zertifikatsspezifikation und -registrierung. Der Aussteller kann die Namen der Profile ändern und Kenndaten des gewünschten Zertifikats angeben. Hierzu zählen z. B. der Gültigkeitszeitraum, die Verwendung von Schlüsseln, DN-Einschränkungen usw.

Zertifikatsregel. Eine benannte Gruppe mit Regeln, die angibt, ob ein Zertifikat für eine bestimmte Klasse von Anwendungen mit gemeinsamen Sicherheitsanforderungen anwendbar ist. Eine Zertifikatsregel kann z. B. angeben, ob ein bestimmter Zertifizierungstyp dem Benutzer die Ausführung von Transaktionen für Waren innerhalb eines bestimmten Preisbereichs ermöglicht.

Zertifikatswiderrufsliste (CRL). Eine digital unterzeichnete, mit Zeitmarken versehene Liste der Zertifikate, die vom Zertifikatsaussteller (CA) widerrufen wurden. Die Zertifikate in dieser Liste sollten als nicht akzeptierbar behandelt werden. *Siehe auch* Digitales Zertifikat.

Zertifizierung. Der Prozeß, bei dem eine zuverlässige, an der Kommunikation nicht beteiligte Stelle (der Zertifikatsaussteller - CA) einen elektronischen Identitätsnachweis ausstellt, der für die Identität einer Person, eines Unternehmens oder einer Organisation bürgt.

Ziel. Eine benannte oder ausgewählte Datenquelle.

Zugriffssteuerungsliste (ACL). Ein Verfahren, mit dem die Verwendung einer bestimmten Ressource auf berechtigte Benutzer beschränkt werden kann.

Index

Numerische Stichwörter

4758-CA-Profil 6

A

Administrator, den ersten für RA hinzufügen 34
AIX
  sichern 12
  wiederherstellen 12
Aktivitätsbericht 14
Aliasing, IP 75
Allgemeine Erweiterungen 67
Alternativname des Ausstellers, Erweiterung 65
Ändern von Konfigurationsdateien 9
Anschluß 41, 46, 48
  CA-Server 20
  Directory-Server 41
  Prüf-Server 46, 48
  RA-Server 38
ASN.1 76
AuditClient.ini 10, 101
AuditServer.ini 10, 97
Authentifizierung 1

B

Befehle eingeben 5
Befehlszeilendienstprogramme
  Audit Archive and Sign 52
  Audit Integrity Check 53
  CA Certification 25, 28, 103
  Enable RA Database Encryption 106
  RA User 105
Berichte
  Aktivität 14
  Nutzung 13
Berichte, Prüfung 52
Binden 49

C

CA (Zertifikatsaussteller)
  gegenseitige Zertifizierung 64
  Hierarchien 64
CA-Server
  CRL-Einstellungen ändern 22
  Datenbankintegrität prüfen 24
  Konfigurationsdatei 78
  Protokolle 32
  Sendeaufrufintervall ändern 21
  Status 32
  Überwachter Anschluß 20
  verwalten 19
CAIntegrityCheck, Dienstprogramm 24
CARemac, Dienstprogramm 24
CCITT 76
Change Password, Dienstprogramm 5
Chiffrierschlüssel 69
CRL, Erstellungsintervall 22
CRL, Gültigkeitsdauer 22
CRL (Zertifikatswiderrufsliste) 67
  Einstellungen, ändern 22
  Erstellungsintervall 22
  Gültigkeitsdauer 22
CRL-Verteilungspunkte, Erweiterung 65

D

Dateien, Konfiguration 77
Daten, Prüfdatenbank 113
Datenbankdaten, Prüfung 113
DB2-Datenbanken 73
  Protokolle 59
  Status 57
  verwalten 57
den ersten Registrator hinzufügen 34
DES 61
Dienstprogramme
  Activity Report (Aktivitätsbericht) 14
  Audit Archive and Sign 52, 107
  Audit Integrity Check 53
  Audit Integrity Check, Dienstprogramm 107
  CA Certification 25, 28, 103, 105
  CAIntegrityCheck 24
  CARemac 24
  Change Password 5
  Enable RA Database Encryption 106
  IniEditor 9
  RA User 35
  Trust Authority Control 7
  Usage Report (Nutzungsbericht) 13
Digitale Zertifikate 68
Digitale Zertifizierung 1
Directory 59
Directory-Administratorkennwort 5
Directory-Attribute des Zertifikatsgegenstands, Erweiterung 65
Directory-Server
  Einträge 28, 31
  Informationen 75
  Protokolle 61
  RA-Einstellungen ändern 41
  Server 41
  Status 60
  verwalten 59
DNS-Adressen 26, 30
Domänen, Registrierung 70

E

E-Mail-Adressen 27, 30
Ereignisprotokoll 50
Ereignisse, Prüfung 47, 110
Ereignisse für Prüfadministratoren 72
Erweiterungen
  allgemein 67
Erweiterungen *(Forts.)*
  Anforderungsablauf 67
  Namenseinschränkungen 31
  privat 67
  Standard 65
  Zertifikat 64

F

Fehlerbehebung 120
Fehlerprotokoll 52
Felder, Prüfereignisse 109

G

gegenseitige Zertifizierung 64
Gegenseitige Zertifizierung 25, 68
Gesicherte Kommunikation 1
Grundlegende Einschränkungen, Erweiterung 65
Gültigkeitsprüfung, Unterschrift 69

H

Hierarchie 28
Hierarchien, CA 64
Hinzufügen von Registratoren 34
Host-Name 41, 46
HTTP Server 17
  Protokolle prüfen 19
  Status 17
  verwalten 17

I

IBM HTTP Server 17, 74
IBM SecureWay 4758 PCI Cryptographic Coprocessor 61, 70
  klonen 12
  Verschlüsselungskoprozessor 70
  verwalten 61
IBM WebSphere Application Server 74
  Protokolle 16
  Status 16
  verwalten 16
ICL (Issued Certificate List) 69
  Schutzregel 23
  Schutzschlüssel 24
Informationszugriff für Aussteller, Erweiterung 65
IniEditor-Dienstprogramm
  Abschnitt hinzufügen 11
  ausführen 9
  Datei speichern 11
  Parameter editieren 11
  Parameter hinzufügen 11
  verwenden 10
Integrität 69
Integritätsprüfung 24, 53, 73
Integritätsversiegelung 73

IP-Adressen, ändern 11
IP-Adreßmaske 26, 29
IP-Aliasing 75
ISO 76
Issued Certificate List (ICL) 69
ITU-Standard 65, 76

J

jonahca.ini 10, 78
jonahra.ini 10, 87

K

Kennwort für Steuerprogramm 5
Kennwörter
  4758-CA-Profil 6
  ändern 5
  Directory-Administrator 5
  Prüfadministrator 5
  Steuerprogramm 5
Klonen des IBM SecureWay 4758 PCI Cryptographic Coprocessor 12
Kommunikation, gesicherte 1
Komponenten, Trust Authority
  CA-Server 20
  IBM HTTP Server 17
  IBM SecureWay 4758 PCI Cryptographic Coprocessor 61
  IBM SecureWay Directory 59
  Prüf-Server 42
  RA-Server 33
  Starten des Servers 7
  Stoppen des Servers 7
  WebSphere Application Server 16
Konfigurationsdatei 10, 77
Konfigurationsdateien
  ändern 9
  AuditClient.ini 101
  AuditServer.ini 97
  CA-Server 78
  jonahca.ini 78
  jonahra.ini 87
  Prüf-Client 101
  Prüf-Server 97
  RA-Server 87

L

LDAP, (Lightweight Directory Access Protocol) 59

M

MAC-Schlüssel 69

N

Nachrichten, PKIX 63
Nachrichtenauthentifizierungscode (MAC) 64
Name des Zertifikatsgegenstands, Erweiterung 65
Namenseinschränkungen, Erweiterung 31, 65
Nutzungsbericht 13
Nutzungszeitraum für privaten Schlüssel, Erweiterung 65

O

Objektkennungen (OID) 76

P

PKIX-Nachrichten 63
Private Erweiterungen 67
Protokolle
  CA-Server 32
  DB2 59
  Directory-Server 61
  Ereignis 50
  Fehler 52
  HTTP Server 19
  Prüf-Server 56
  Prüfsubsystem 52
  Prüfung 49, 50
  RA-Server 39
  Trace 51
  WebSphere Application Server 16
Prüfadministratorkennwort 5
Prüfen der Protokolle des HTTP Servers 19
Prüfereignis 110
  Ereignisse für Prüfadministratoren 72
  Masken 72
  RA 72
  Schlüsselverwaltung 72
  sicherheitsrelevant 72
  verbindlich 73
  wahlfrei 73
  Zertifikatsverwaltung 72
Prüfmaske 47
Prüfprotokolltabelle 117
Prüfsubsystem
  Ändern der Protokolleinstellungen 50
  Anschluß ändern 48
  Audit Archive and Sign, Dienstprogramm 107
  Audit Integrity Check, Dienstprogramm 107
  Client-Konfigurationsdatei 101
  Datenbanksichten 43
  Datensätze, Informationen zu 72
  Ereignismasken 72
  Ereignisse, Informationen 72
  Fehlerprotokolleinstellungen ändern 52
  Host-Name ändern 47
  Informationen 71
  Intervall zwischen Wiederholungsversuchen ändern 48
  Protokolldateien, Archiv 52
  Protokolldateien, unterzeichnen 52
  Protokolle 49, 56
  Prüfmaske ändern 47
  Prüfprotokolleinstellungen ändern 50
  Server-Konfigurationsdatei 97
  Status 55
  Trace-Protokolleinstellungen ändern 51
Prüfsubsystem *(Forts.)*
  verbindliche Ereignisse 73
  verwalten 42
  wahlfreie Ereignisse 73
Prüfung
  Anschluß ändern 46, 47
  Berichte generieren 52
  Bindungsversuche ändern 49
  Datenbankdaten 113
  Host-Name ändern 46
  Intervall zwischen Bindungsversuchen ändern 49
  Intervall zwischen Wiederholungsversuchen ändern 48
  Maske 47
  Protokoll 50
  Protokolleinträge suchen 46
  Prüfereignisse, Felder 109

Q

Quellentabelle 115

R

RA (Registrierungsstelle)
  Add RA User, Dienstprogramm 105
  Administrator hinzufügen 35
  Administratoren (Registratoren) 70
  den ersten Administrator hinzufügen 34
  den ersten Registrator hinzufügen 34
  Dienstprogramm Add RA User 35
  Informationen 70
RA-Ereignisse 72
RA-Server 33
  Anschluß des Directory ändern 41
  Datenbankverschlüsselung aktivieren 37, 106
  Host-Name des Directory ändern 41
  Konfigurationsdatei 87
  Protokolle 39
  Sendeaufrufintervall ändern 38
  Status 39
  überwachten Anschluß ändern 38
  verwalten 33
  Wiederholungsintervall ändern 39
Regeleinschränkungen, Erweiterung 65
Regelzuordnung, Erweiterung 65
Registratoren hinzufügen 34
Registrierter Name (DN) 69
Registrierungsdomänen 70
RFC 2459 65
RSA 61

S

Schlüssel
  MAC 69
  Verschlüsselung 69
Schlüsselkennung des Ausstellers, Erweiterung 65
Schlüsselkennung des Zertifikatsgegenstands, Erweiterung 65
Schlüsseltabelle 114
Schlüsselverwaltungsereignisse 72
Schlüsselverwendung, Erweiterung 65

Schutz
Regel, ICL 23
Schlüssel, ICL 24
Schutzregel, ICL 23
Sendeaufrufintervall 21, 38
Sendeintervall 41
Server
CA-Server 19
Directory 41, 75
HTTP 17, 74
IBM WebSphere Application Server 74
Komponenten starten 7
Komponenten stoppen 7
Prüfung 42
RA 33
Web 74
WebSphere Application 16
Sicherheit, Trust Authority 63
Sicherheitsrelevante Ereignisse 72
Sicherung 12
AIX 12
Trust Authority-Datenbanken 12
Windows NT 12
Sichten, Prüfdatenbank 43
Smart Cards 71
SQL-Befehl 35
Standarderweiterungen 65
Standards
ASN.1 76
CCITT 76
ISO 76
ITU 65, 76
RFC 2459 65
X.509v3 65
X.680 76
Starten von Server-Komponenten 7
Status
CA-Server 32
DB2-Datenbanken 57
Directory-Server 60
HTTP Server 17
Prüf-Server 55
RA-Server 39
WebSphere Application Server 16
Stoppen von Server-Komponenten 7
Systemtabelle 118

T

Tabelle der Arten betroffener Entitäten 116
Tabelle der berechtigten Aufgabenbereiche 116
Tabelle der berechtigten Entitäten 115
Tabelle der Komponentenarten 116
Tabelle für Ereignisbewertung 114
Tabelle zur Ereignissteuerung 114
Tabellen, Prüfdatenbanken
berechtigte Aufgabenbereiche 116
berechtigte Entitäten 115
betroffene Entitäten, Tabelle der Arten 116
Ereignisbewertung 114
Ereignissteuerung 114
Komponentenarten, Tabelle 116
Quellen 115
Schlüssel 114
Tabellen, Prüfdatenbanken *(Forts.)*
Tabelle für Prüfprotokoll 117
Tabelle für System 118
Timer 48
Trace-Protokoll 51
Trust Authority
Ändern von IP-Adressen 11
Berichte 13, 14
Beschreibung 1
Sicherheit 63
sichern 12
Steuerung 7
verwalten 5
wiederherstellen 12

U

Überwachter Anschluß 38
Uniform Resource Identifiers (URIs) 27
Unterschrift, Gültigkeitsprüfung 69
Unterzeichnen 69
URIs 31

V

Verschlüsselung für RA-Datenbank aktivieren 37
Verschlüsselungskoprozessor 63
Vertraulichkeit 69
Verwalten
CA-Server 19
DB2 UDB 57
Directory-Server 59
HTTP Server 17
IBM SecureWay 4758 PCI Cryptographic Coprocessor 61
Prüfsubsystem 42
RA-Server 33
Trust Authority 5
WebSphere Application Server 16

W

Web-Server 74
WebSphere Application Server 16
Widerrufsliste (CRL) für Zertifikate 1
Wiederherstellen 12
AIX 12
Trust Authority-Datenbanken 12
Windows NT 12
Wiederholungen 47
Wiederholungsintervall 39
Windows NT
sichern 12
wiederherstellen 12

X

X.509v3 65
X.680 76

Z

Zertifikat
Aktivität überwachen 14
ausstellen 1
Zertifikat *(Forts.)*
Erneuerung 1
Erweiterungen 64
Nutzung überwachen 13
widerrufen 1
Zertifikatswiderrufsliste (CRL) 1, 67
Zertifikate 68
Zertifikatsaussteller (CA) 63
Zertifikatsverwaltungsereignisse 72
Zertifizierung, digitale 1, 68
Zertifizierungsregeln, Erweiterung 65
Zugriffssteuerungsliste (ACL) 63

Antwort

IBM SecureWay Trust Authority
Systemverwaltung
Version 3 Release 1.2

IBM Form SH12-2979-01

Anregungen zur Verbesserung und Ergänzung dieser Veröffentlichung nehmen wir gerne entgegen. Bitte informieren Sie uns über Fehler, ungenaue Darstellungen oder andere Mängel.

Zur Klärung technischer Fragen sowie zu Liefermöglichkeiten und Preisen wenden Sie sich bitte entweder an Ihre IBM Geschäftsstelle, Ihren IBM Geschäftspartner oder Ihren Händler.

Unsere Telefonauskunft ″HALLO IBM″ (Telefonnr.: 01803/31 32 33) steht Ihnen ebenfalls zur Klärung allgemeiner Fragen zur Verfügung.

Kommentare:

Danke für Ihre Bemühungen.

Sie können ihre Kommentare betr. dieser Veröffentlichung wie folgt senden:
- Als Brief an die Postanschrift auf der Rückseite dieses Formulars
- Als E-Mail an die folgende Adresse: comment@tcvm.vnet.ibm.com

Name	Adresse
Firma oder Organisation	
Rufnummer	E-Mail-Adresse

Antwort
SH12-2979-01

IBM

IBM Deutschland Informationssysteme GmbH
SW NLS Center

70548 Stuttgart

Programmnummer: 5648-D09

Printed in Denmark

SH12-2979-01